VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Síťová virtualizace v počítačových sítích

Network Virtualization in Computer Networks

2019 František Urbánek

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. František Urbánek**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Síťová virtualizace v počítačových sítích
Network Virtualization in Computer Networks

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování různých způsobů síťové virtualizace v počítačových sítích v laboratorním prostředí s využitím přepínačů a směrovačů Cisco a Huawei.

Osnova práce:
1. Popište různé způsoby virtualizace v počítačových sítích.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři způsoby využití virtualizace v počítačových sítích. Použijte k tomu přepínače a směrovače Cisco a Huawei. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu přepínačů a směrovačů Cisco a Huawei v těchto sítích.
4. Srovnejte jednotlivá řešení. Zhodnoťte výhody a nevýhody jejich použití.

Seznam doporučené odborné literatury:

[1] TEARE, Diane, et al. *CCNP Routing and Switching Foundation Learning Library: Foundation Learning for CCNP ROUTE, SWITCH, and TSHOOT (642-902, 642-813, 642-832).* 1st ed. Indianapolis: Cisco Press, 2010. ISBN-13: 978-1-58705-885-1.
[2] MIR, Nader F. *Computer and Communication Networks.* Upper Saddle River, NJ: Prentice Hall, 2015. ISBN 9780133814743.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2017

Datum odevzdání: 30.04.2019

prof. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prehlasujem, že som túto prácu vypracoval samostatne. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal.

V Ostrave 29. Apríla 2019

.....

V prvom rade by som rád poďakoval Ing. Petrovi Machníkovi, Ph.D. za zaujímavú tému diplomovej práce, vďaka ktorej som sa mohol oboznámiť s novými technológiami a platformami, ďalej za odborné vedenie mojej práce a efektívne konzultácie, aj vďaka ktorým sa mi podarilo prácu úspešne dokončiť.

Ďalej by som sa rád poďakoval Ing. Pavlovi Nevludovi, za poskytnutie všetkých prostriedkov na učebni POREB215, ktoré boli nutné pri vypracovávaní tejto práce a taktiež za cenné rady a informácie ktoré taktiež významne prispeli ku úspešnému dokončeniu práce.

Abstrakt

Práca sa zaoberá rozborom a realizáciou spôsobov virtualizácie, bežne používaných v počítačových sieťach, za využitia platforiem Cisco a Huawei, vzájomné porovnanie týchto dvoch platforiem a ich spoluprácu a možnosti nasadenia pri rozoberaných virtualizačných technikách.

Práca obsahuje rozbor a popis funkčnosti jednotlivých virtualizačných techník a ich následnú konfiguráciu, pričom pri všetkých technológiách je uvedený podrobný postup ich konfigurácie na oboch platformách. V práci je ďalej obsiahnuté testovanie funkcionality týchto virtualizačných techník za použitia oboch platforiem a overenie ich vzájomnej spolupráce a kompatibility v aktívnej počítačovej sieti, čo bolo jedným s cieľov tejto diplomovej práce.

Klíčová slova: Cisco, EtherChannel, Huawei, InterVLAN Routing, MPLS, počítačové siete, virtualizácia, VLAN, VRRP

Abstract

Thesis is dealing with analysis and realization of virtualization techniques, which are comonly used in computer networks, using the Cisco and Huawei platforms, comparison of these two platforms and their cooperation and possibilities of deployment.

Thesis includes analysis and description of functionality of every single virtualization technique this thesis is dealing with, folowing the detailed process of their configuration on both platforms. Thesis also contains the testing of functionality of these virtualization techniques while using both platforms in active network deployement and checking their mutual compatibility, which was one of the goals of this thesis.

Key Words: Cisco, computer networks, EtherChannel, Huawei, InterVLAN Routing, MPLS, virtualization, VLAN, VRRP

Obsah

Seznam použitých zkratek a symbolů

ASN	–	Autonomous System Number
ATM	–	Asynchronous Transfer Mode
BGP	–	Border Gateway Protocol
BW	–	Bandwith
C	–	Customer
CE	–	Customer Edge
CEF	–	Cisco Express Forwarding
EIGRP	–	Enhanced Interior Gateway Routing Protocol
GRE	–	Generic Routing Encapsulation
IEEE	–	Institute of Electrical and Electronics Engineers
IP	–	Internet Protocol
IETF	–	Internet Engineering Task Force
IOS	–	Internetwork Operating System
IPsec	–	Internet Protocol Security
ISO	–	International Organization for Standardization
LACP	–	Link Aggregation Control Protocol
LACPDU	–	Link Aggregation Control Protocol Data Unit
LDP	–	Label Distribution Protocol
LFIB	–	Label Forwarding Information Base
LSP	–	Label Switched Path
LSR	–	Label Switching Router
MAC	–	Media Access Contro
MD5	–	Message Digest 5
MP-BGP	–	Multiprotocol Border Gateway Protocol
MPLS	–	Multiprotocol Label Switching
NIC	–	Network Interface Card
OSI	–	Open Systems Interconnection
OSPF	–	Open Shortest Path First
P	–	Provider
PAgP	–	Port Aggregation Protocol
PE	–	Provider Edge
PVC	–	Permanent Virtual Circuit
RD	–	Route Distinguisher
RFC	–	Request for Comments
RT	–	Route Target
SPOF	–	Single Point of Failure

SVI	–	Switched Virtual Interface
TPID	–	TextProtocolIdentifier
UTP	–	Unshielded Twisted Pair
VLAN	–	Virtual Local Area Network
VPLS	–	Virtual Private LAN Service
VPN	–	Virtual Private Network
VRF	–	Virtual Route Forwarding
VRP	–	Versatile Routing Platform
VRRP	–	Virtual Router Redundancy Protocol

Seznam obrázků

1 Úvod

Už po vzniku prvých počítačov bola potreba tieto počítače medzi sebou prepájať za účelom výmeny informácií, čo bolo podnetom pre vznik počítačových sietí. Postupom času sa počítačové siete stále rozrastali a začali sa rozdeľovať podľa ich účelu. Takmer v každej spoločnosti od menších až po veľké korporácie bolo potrebné navrhnúť a implementovať vhodné sieťové riešenie. Navrhnutú sieť však bolo potrebné časom stále rozširovať, či už o nové podsiete, servery alebo užívateľské počítače. Takéto rozširovanie sa postupne začalo stávať nepraktickým z kapacitného a rozpočtového hľadiska, preto museli inžinieri z inštitútu pre elektronické a elektrotechnické inžinierstvo prísť s riešeniami ktoré by takéto problémy odstránilo. Riešenia nakoniec začali prichádzať postupne v podobe noriem popisujúcich rôzne metódy virtualizácie v počítačových sieťach, kedy popri fyzickej topológie siete pribudla taktiež aj logická topológia. Virtualizačné technológie sa časom stali kľúčovými prvkami pri stavbe počítačových sietí v spoločnostiach po celom svete.

Novým normám, ktoré popisovali rôzne virtualizačné technológie, sa museli prispôsobiť hlavne výrobcovia prvkov počítačových sietí, ktorí svoje zariadenia a operačný systém museli prispôsobiť používaniu nových technológií. Popri veľkých spoločnostiach ako je napríklad Cisco Systems sa na sieťovom trhu postupne začali objavovať aj ďalšie menšie firmy, ktoré sa snažili týmto veľkánom konkurovať formou poskytnutia lacnejšej alternatívy pre potencionálnych zákazníkov.

Cieľom tejto diplomovej práce bolo popísať rôzne virtualizačné technológie bežne používané v praxi a následne ich implementovať za využitia dvoch rozdielnych platforiem od spoločností Cisco System a Huawei. Oproti spoločnosti Cisco, ktorá je popredným výrobcom sieťových prvkov, je spoločnosť Huawei v odvetví počítačových sietí menej populárna. V práci sú pri implementácii jednotlivých virtualizačných technológií nasadené obe tieto platformy, za účelom overenia ich spolupráce a funkcionality implementovanej technológie. Práca teda popisuje možnosť implementácie platformovo nehomogénnej siete a oboznamuje užívateľa s oboma platformami, postupom konfigurácie jednotlivých technológií na oboch platformách a rozdielmi v ktorých sa jednotlivé platformi líšia.

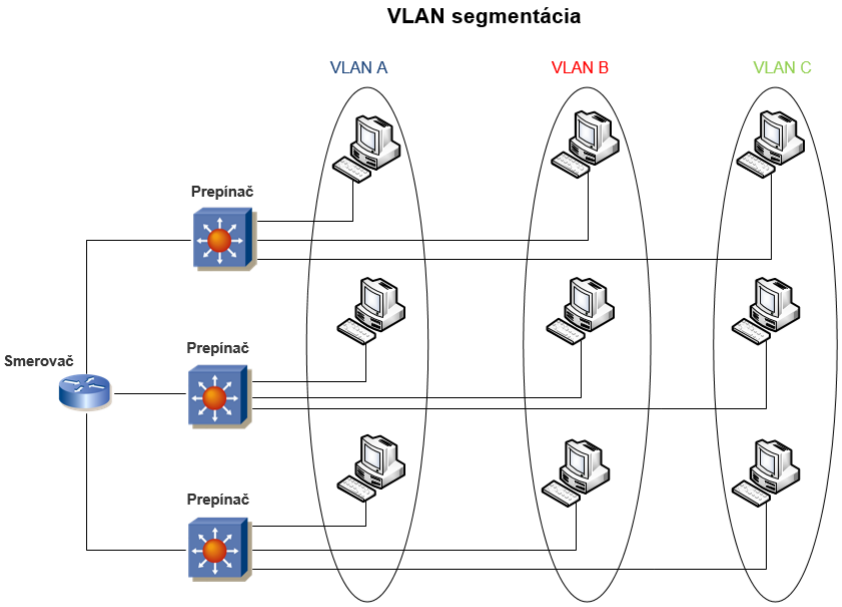
V úvode práce sa čitateľ zoznámi s jednotlivými virtualizačnými technológiami, ktoré sú v práci rozoberané. V praktickej časti sa potom stretne so spôsobom realizácie týchto technológií v bežných sieťových riešeniach na oboch platformách a na záver sa dozvie o drobných rozdieloch medzi oboma platformami, na ktoré si treba dať pozor pri ich spoločnom nasadení v praxi.

2 Virtuálne lokálne počítačové siete(VLAN)

VLAN alebo taktiež virtuálna LAN slúži k logickému rozdeleniu siete nezávisle na fyzickom usporiadaní, teda administrátor je schopný segmentovať sieť na menšie siete vo vnútri fyzickej štruktúry pôvodnej siete. Požiadavok na VLAN siete vznikol hlavne kvôli rozrastajúcim sa sieťovým infraštruktúram (vo firmách, školách, rôznych spoločnostiach atd.) a kvôli požiadavku deliť sieť pomocou logického delenia namiesto fyzického, pri ktorom sa prejavuje množstvo obmedzení ako napríklad pripojenie koncových staníc na určitý fyzický segment. Pri VLAN sieťach nie sme obmedzený hardvérovou kapacitou a za predpokladu že operačný systém prepínača pracuje bezchybne , neexistuje žiadny spôsob akým by sa rámec, ktorý pochádza z jednej siete VLAN, dostal do inej siete VLAN.

Vďaka VLAN sieťam je možné rozdeliť broadcastovú doménu na niekoľko logicky oddelených domén a zamedziť tak nadbytočnej prevádzke pri broadcastoch. Na to aby bolo možné jednotlivé VLAN siete prepojiť je potreba smerovač(alebo prepínač podporujúci L3), bez ktorého by komunikácia medzi užívateľmi z rozdielnych VLAN sietí nebola možná.

S VLAN sieťami teda môže administrátor pracovať ako s bežnými LAN sieťami, napríklad použiť medzi nimi akýkoľvek typ smerovania, kontrolovať komunikáciu medzi týmito sieťami a využívať všetky vlastnosti, ktorými LAN siete disponujú, bez nutnosti obmedzovať sa na fyzický segment. Jednotlivé VLAN môžu byť prepojené aj vertikálne a je teda možné rozdeliť určitú sieť z hľadiska účelu anie podľa fyzického umiestnenia.



Obrázek 1: Príklad modelu VLAN siete

2.1 Delenie VLAN sietí

V praxi je VLAN siete možné deliť z hľadiska ich konfigurácie na dva typy:

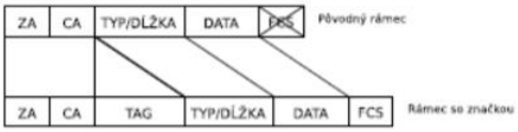
- **Statické VLAN** – Pri tomto typu VLAN sietí administrátor priraďuje jednotlivým portom na prepínači príslušnú VLAN sieť staticky. Ak je do tohoto portu pripojené nejaké zariadenie tak spadá do VLAN siete, ktorá je tomuto portu priradená. Určitou nevýhodou toho typu VLAN sietí je to, že pri potrebe zmeniť stávajúcu VLAN konfiguráciu na prepínači je administrátor nutný sa na toto zariadenie prihlásiť a zmeny uskutočniť manuálne.
- **Dynamické VLAN** – Pri tomto typu VLAN sietí je nutné použitie určitého kontroléra (tzv. VLAN Management Policy server), ktorý spravuje viacero prepínačov a priraďuje nastaveným VLAN sieťam určité porty, na základe zariadenia, ktoré je do určitého portu pripojené. Tento kontrolér je teda schopný koncové zariadenie identifikovať na základe jeho MAC adresy a určiť do akej VLAN siete patrí a tým pádom do akej VLAN siete patrí port na prepínači, do ktorého je toto koncové zariadenie pripojené. Pri dynamických VLAN sieťach je možné koncové zariadenia identifikovať aj napríklad pomocou adresy podsiete, pričom na priradenie zariadenia do VLAN sa použije jeho IP adresa z hlavičky datagramu. Taktiež je možné zariadenie identifikovať pomocou protokolu a to aj na základe protokolu vyšších vrstiev, napríklad podľa použitého protokolu. Zariadenia využívajúce určitý protokol (napr. smtp) môžu byt zaradené do odlišnej VLAN ako zariadenia využívajúce protokol iný (napríklad https).

2.2 Identifikácia účastníkov VLAN

V prípade, že je vrámci viacerých VLAN sietí použitých niekoľko prepínačov, je potrebné rozlíšiť do ktorej VLAN daný datagram patrí. Toto rozlišovanie sa robí pomocou rámcov, do ktorých sa vloží identifikačná značka jedinečná pre každú VLAN sieť. Všetok prenos vrámci jednej VLAN je teda pomocou jednotky prenosu na linkovej vrstve (rámcom), označený pomocou určitej značky na základe ktorej prepínače zistia do akej VLAN siete táto komunikácia patrí. Táto značka sa do rámca umiestňuje pred vstupom do tzv. trunku, čo je v podstate prepoj medzi dvoma prepínačmi, ktorým prúdi komunikácia z viacerých VLAN sietí. Administrátor je schopný do tohoto trunku vkladať VLAN siete a tak kontrolovať z ktorej VLAN siete má prepínač prenos prepustiť a z ktorej naopak zahodiť. Až sa datagram napokon dostane ku cieľovému zariadeniu tak sa táto značka z rámca odstráni.

2.3 Značkovanie rámcov

Prideľovanie značiek jednotlivým rámcom je vykonávané podľa protokolu IEEE 802.1Q , ktorý je založený na vkladaní značky do hlavičky daného rámca. Na obrázku 2 je zobrazený pôvodný rámec a rámec obohatený značkou (TAG).



Obrázek 2: Pôvodný rámec a rámec so značkou

Počet bitov	16	3	1	12
Časť značky	TPID	Priorita	CFI	VLAN ID

Obrázek 3: Značka protokolu 802.11Q

Prvých 16 bitov je vyhradených pre TPID (Text Protocol Identifier), ktorý určuje typ značky. Ďalšie 3 bity sú určené pre prioritu a nasledujúci 1 bit pre CFI (Canonical Format Identifier). Tento bit sa používa pre kompatibilitu s Token Ring protokolmi, pričom ak je jeho hodnota 0, znamená to že MAC adresa je v nekanonickom formáte a ak je táto hodnota iná než 0, znamená to že MAC adresa je v kanonickom formáte. Posledných 12 bitov je určených pre identifikátor VLANy, teda slúži na určenie príslušnosti rámca k danej VLAN sieti. Teoreticky teda môže byť na základe veľkosti identifikátora maximálny počet VLAN 4096.

2.4 Výhody VLAN

Virtuálne LAN siete prinášajú veľké množstvo výhod ako sú:

- Zvýšenie bezpečnosti – Komunikácia je izolovaná v rámci VLAN siete čo umožňuje ľahšiu kontrolu prevádzky z hľadiska administrácie.
- Zvýšená priepustnosť a výkon siete – Sieť je logicky segmentovaná, čo sa odrazí na prenosovej kapacite, ktorá sa delí medzi koncovými stanicami. Menej koncových staníc znamená zvýšenie priepustnosti a redukciu vyťaženie siete spôsobovanej broadcast správami.
- Nezávislosť na fyzickej topológii – Obrovská výhoda, ktorá spočíva v logickom delení siete nezávisle na fyzickú infraštruktúru. V praxi to znamená, že vo fyzickej infraštruktúre siete, ktorá už je navrhnutá a postavená nemusia byť prevádzané žiadne zmeny. Stačí len upraviť konfiguráciu na smerovačoch a prepínačoch a sieť rozdeliť na logické segmenty.
- Jednoduchá administrácia siete – Jednoduchá zmena konfigurácie VLAN siete a jednoduché pridávanie staníc v rámci siete, činí VLAN siete nenáročné na spravovanie aj pre menej skúseného technika.
- Šetrenie finančných prostriedkov na infraštruktúru.

2.5 Virtuálne rozhranie SVI a InterVLAN smerovanie

SVI(Switched Virtual Interface)je logické rozhranie, ktoré sa konfiguruje na multi-vrstvovom prepínači. Toto logické rozhranie môže byť vytvorené pre každú VLAN sieť existujúcu v sieti, pričom konkrétnemu SVI môže byť priradená len jedna VLAN sieť. SVI je virtuálny port, ktorý poskytuje pre VLAN sieť rovnakú funkcionalitu ako rozhranie smerovača a môže byť v podstate nakonfigurovaný obdobne ako rozhranie smerovača. Inými slovami SVI pre VLAN sieť poskytuje spracovanie tretej vrstvy ISO OSI modelu pre všetky pakety prichádzajúcich z alebo do portov priradených ku danej VLAN sieti.

Výhoda SVI spočíva hlavne v tom, že pre komunikáciu účastníkov z rôznych VLAN nie je nutné používať takzvané „router on the stick“ zapojenie, ktoré je pomalšie ako využitie SVI. Dáta sa smerujú medzi VLAN sieťami priamo na L3 prepínači a nemusia ísť až na smerovač. Takémuto typu smerovania dát sa hovorí InterVLAN smerovanie.

Použitie SVI taktiež odstraňuje SPOF(Single point of failure), ktorý sa vyskytuje pri použití „router on the stick“ metódy. Kedže SVI je virtuálne, vyhneme sa možným chybám, ktorý by mohli vzniknúť na fyzickej linke medzi prepínačom a smerovačom.

Nevýhoda SVI spočíva hlavne v cene multi-vrstvových prepínačov, ktoré sú o dosť drahšie ako klasický L2 prepínač spolu s lacnejším smerovačom.

3 Agregácia liniek - EtherChannel

Agregácia liniek je označenie pre technológiu, ktorá umožňuje agregovať (spájať) viacero fyzických liniek do jednej virtuálnej za účelom navýšenia priepustnosti a redundancie daného spojenia. Táto technológia je popísaná v norme IEEE 802.3ad a existuje jej niekoľko proprietárnych variant ako:

- EtherChannel - Cisco
- Aggregated Ethernet - Juniper
- EtherTrunk - Huawei
- Multi-Link Trunking - AVAYA

Pojem EtherChannel sa teda vyskytuje hlavne v Cisco terminológii a je to označenie pre technológiu umožňujúcu agregáciu liniek(spájanie ethernetových rozhraní)na prepínačoch, smerovačoch a serverov. Táto technológia sa primárne používa medzi prepínačmi ale môže sa použiť aj pre pripojenie serveru ku prepínači, v tomto prípade hovoríme o pojme NIC(Network Interface Card)Teaming alebo NIC bonding.

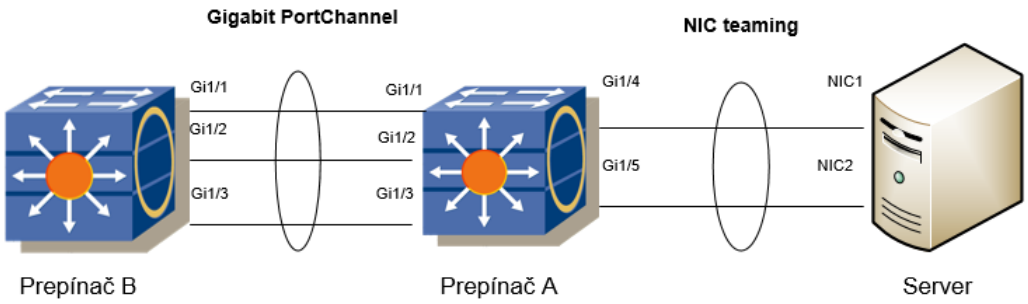
EtherChannel zabezpečuje prijímanie a odoslanie dát cez viacero fyzických rozhraní. Za pomoci protokolov ako LACP alebo PAgP sa vyjedná a vytvorí tzv. PortChannel, pričom počet fyzických rozhraní zahrnutých do PortChannelu môže byť 2 až 8 pre PAgP a až 16 rozhraní pre LACP. Vytvorený PortChannel je virtuálny port, s ktorým potom pracujú všetky ostatné technológie ako napríklad Spanning tree. Ten miesto skupiny portov vidí len jeden virtuálny a nedochádza tak k prípadnému blokovaní týchto portov. Aby mohli byť rozhrania pridané do PortChannelu musia spĺňať následujúce parametre:

- Rozhrania musia byť rovnakého typu.
- Rozhrania musia mať rovnakú prenosovú rýchlosť.
- Rozhrania musia byť zaradené do rovnakej VLANy alebo do trunk módu z rovnakými parametrami.

EtherChannel využíva pre prerozdeľovanie záťaže medzi jednotlivými linkami PortChannelu tzv. Load Balancing. Pri odosielaní dát sa podľa MAC adresy a zdrojovej či cieľovej IP adresy rozhodne akou linkou sa dáta odošlú, pričom je snaha o uchovanie rámcov z jedného spojenia v rovnakej linke aby nedochádzalo k doručovaniu rámcov mimo poradia a iným problémom. Prichádzajúce dáta sa zo všetkých rozhraní združujú do virtuálneho portu. V prípade výpadku jednej linky sa aktívne spojenie presunie na niektorú zo zostávajúcich liniek, pričom dané spojenie sa nepreruší a dôjde približne len ku sekundovému oneskoreniu.

EtherChannel môže fungovať za využitia dvoch protokolov:

1. PAgP(Cisco Port Aggregation Protocol) - Cisco proprietárny protokol, ktorý je podporovaný výlučne na prepínačoch spoločnosti Cisco. PortChannel môže byť vytvorený len z rozhraní na jednom prepínači, nie na tzv. stacku (jedná sa o zoskupenie viacerých fyzických zariadení ktorá logicky pôsobia ako jedno zariadenie). PAgP môže pracovať v dvoch módoch:
   - Desirable - prepínač sa aktívne snaží vyjednať zostavenie EtherChannelu.
   - Auto - EtherChannel sa začne zostavovať len ked prepínač obdrží požiadavok z vonku.
2. LACP(Link Aggregation Control Protocol) - LACP je štandardizovaný protokol, ktorý je oproti PAgP možno použiť aj na prepínačoch od iných výrobcov ako Cisco. Obdobne ako PAgP aj tento protokol pracuje v dvoch módoch:
   - Active - prepínač sa snaží automaticky nadviazať EtherChannel spojenie odosielaním LACP paketov.
   - Passive - prepínač čaká na začiatok vyjednávania EtherChannelu zvonku.



Obrázek 4: Príklad použitia technológie EtherChannel

3.1 NIC Teaming

NIC Teaming je formou EtherChannelu, vďaka ktorej môžeme spojiť dva alebo viac fyzických NIC(sieťových kariet) do jedného logického sieťového adaptéru, ktorý sa označuje ako

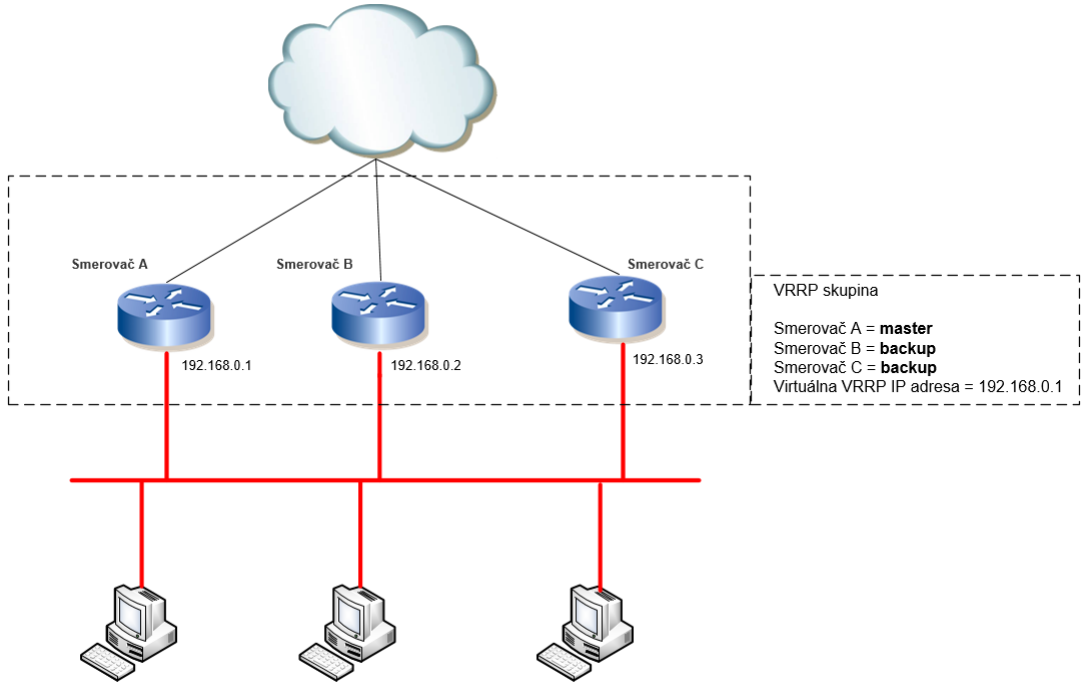
bond(zväzok). Pri použití správneho ovládača pre sieťovú kartu je možné na tejto karte konfigurovať VLANy a NIC teaming. Pomocou VLAN je možné jeden fyzický adaptér rozdeliť na viacero virtuálnych a naopak pomocou NIC teamingu je možné viacero fyzických adaptérov spojiť do jedného logického. Vytvorením NIC zväzku sa vytvorí jedno virtuálne rozhranie, ktoré získa svoju MAC adresu z jedného fyzických rozhraní a môže mu byť nastavená jedna alebo viacej IP adries. NIC Teaming môže taktiež fungovať aj s obyčajným hubom, ktorý nepodporuje Agregáciu liniek. V tomto prípade sa konfiguruje iba na serverovej strane a primárne sa uplatňuje len na odchádzajúci prevoz.

Pri nastavovaní teamingu je možné voliť z viacerých metód alebo typov:

- **Adapter Fault Tolerance** - Jeden adaptér je aktívny a ostatné sú standby(prepnú so do active v prípade výpadku). Pri tomto móde nie je potreba nič nastavovať na strane prepínača.
- **Switch Fault Tolerance** - Podporuje dve linky pripojené do dvoch rôznych prepínačov, pričom jedna linka je aktívna a druhá standy. Pri tomto móde nie je potreba nič nastavovať na strane prepínača.
- **Adapative Load Balancing** - Odosielaný prevoz sa vyvažuje cez všetky sieťové adaptéry a zároveň sa poskytuje Fault Tolerance(vlastnosť, ktorá umožňuje systému fungovať naďalej aj v prípade zlyhania nejakej jeho súčasti). Pri tejto metóde je možné aplikovať Load Balancing aj na prichádzajúcom prevoze. Obdobne ako pri predchádzajúcich dvoch metódach, nie je potreba nič nastavovať na strane prepínača.
- **Static Link Aggregation** - Použitie manuálneho EtherChannelu kedy je na prepínači nastavený mód On.
- **Dynamic Link Aggregation** - využíva sa LACP protokol.

4 Virtual Router Redundancy Protocol(VRRP)

VRRP je protokol počítačových sietí vďaka ktorému je možné preniesť povinnosti aktívneho sieťového prvku, ktorý zastáva funkciu východzej brány, na iný aktívny prvok. V praxi sa často stáva, že smerovač slúžiaci ako východzia brána pre lokálnu sieť, či už kvôli softvérovej, hardvérovej či inej poruche vypadne. Aby sa v prípade tejto situácie vyhlo kompletnému výpadku pre sieť pripojenej ku tomuto smerovaču, je nutné zabezpečiť určitú formu redundancie, ktorá by umožnila sekundárnemu smerovaču prebrať funkciu primárneho. Pomocou VRRP je možné vytvoriť jednu alebo viac tzv. VRRP skupín, v rámci ktorých môže viacero smerovačov zdieľať jednu virtuálnu IP adresu, ktorá slúži ako východzia brána pre určitú lokálnu sieť. Z hľadiska lokálnej siete sa teda používa len jedna virtuálna IP adresa ako východzia brána, reálne sa však za touto IP adresou môže skrývať viacero aktívnych prvkov.



Obrázek 5: Príklad použitia technológie VRRP

Virtuálna IP adresa pre VRRP skupinu môže byť aj adresa fyzického rozhrania jedného zo smerovačov VRRP skupiny ako je tomu aj napríklad na obrázku 5. V tomto prípade smerovač s touto IP adresou preberá automaticky úlohu master. Obecne sa o tom, ktorý smerovač prevezme úlohu master smerovača rozhoduje pomocou tzv. priority. Smerovač s najväčšou prioritou vo VRRP skupiny sa stáva mastrom. Priorita sa môže na každý smerovač nastaviť manuálne v prípade, že chceme mať kontrolu nad tým, ktorý smerovač bude master, ktorý smerovač prevezme úlohu mastra v prípade výpadku atď. . Predvolene má každý smerovač prioritu 100, ak má

smerovač rovnakú IP adresu rozhrania akou je VRRP ip adresa, dostáva prioritu 255, čo je maximálna možná priorita. V prípade, že majú smerovače rovnakú prioritu, sa rozhoduje o master smerovači porovnaním ich primárnych IP adries, pričom ten s najväčšou vyhráva.

Hlavný smerovač v skupine posiela ostatným smerovačom tzv. VRRP správy(predvolene každú sekundu ak sa nenastaví inak), v ktorých informuje o svojej priorite a taktiež aj o tom, že je stále aktívny. Ostatné smerovače tieto správy počúvajú a porovnávajú prioritu hlavného smerovača so svojou. V prípade, že je priorita obsiahnutá v správe vyššia ako ich vlastná tak sa nič nedeje, v opačnom prípade začnú posielať svoje vlastné VRRP správy, v ktorých informujú o svojej priorite. VRRP správy sa zasielajú na multicast adresu pre VRRP - **224.0.0.18** pre ipv4 a **FF02:0:0:0:0:0:0:12** pre ipv6. Záložné smerovače považujú hlavný smerovač za nedostupný ak od neho neobdržia žiadnu správu po dobu dlhšiu ako tri krát časový interval pre VRRP správy. Pri výpadku master smerovača preberá jeho funkciu smerovač s druhou najväčšou prioritou. Situáciu, v ktorej sa pôvodnému master smerovaču navráti jeho funkcionalita rieši tzv. VRRP "preemption", pričom ak je zapnutý, tak sa mu rola master navráti. Dobu kedy pôvodný master znovu prevezme svoju rolu je možné manuálne predĺžiť, napríklad ak chceme aby mal dostatok času plne obnoviť svoju celkovú funkcionalitu(naplnenie smerovacích tabuliek atď.).

4.1 Výhody VRRP

Používanie protokolu VRRP v počítačovej sieti má viacero výhod, ako napríklad:

- **Redundancia** - VRRP umožňuje spájať viacero smerovač do jednej východzej brány a redukuje tak možnosť SPOF(Single point of failure) v počítačovej sieti.
- **Zdieľanie záťaže** - Konfigurácia VRRP umožňuje zdieľať dáta z klientských staníc medzi všetky dostupné smerovače a teda efektívne rozložiť záťaž medzi týmito smerovačmi.
- **Viacero VRRP skupín** - VRRP podporuje až 255 VRRP skupín na jednom smerovači a 4 pre každé fyzické rozhranie môžu existovať až 4 VRRP skupiny. Práve vďaka podpore viacero VRRP skupín pre rozhranie je možné implementovať zdieľanie záťaže.
- **Preemption** - Funkcia VRRP preemption umožňuje bývalému master smerovači opätovne prebrať jeho master úlohu potom čo sa jeho funkcionalita obnoví. Doba po ktorej sa funkcionalita bývalého master smerovača obnoví je konfigurovateľná podľa potrieb užívateľa.
- **Funkcia Object tracking** - Object tracking umožňuje ovplyvňovať VRRP prioritu pre smerovače vo VRRP skupine sledovaním ich objektov. Za objekt môžeme považovať napríklad rozhranie smerovača, prípadne určité smerovacie parametre. Pomocou tejto funkcie je užívateľ schopný ovplyvňovať prioritu jednotlivých smerovač na základe viacerých parametrov ako len ich dostupnosti.

- **Adresovanie správ** - VRRP používa pre adresovanie správ dedikovanú IANA(Internet Assigned Numbers Authority) multicast adresu - **224.0.0.18** čo výrazne zlepšuje identifikáciu VRRP packetov v sieťovom segmente.
- **Autentifikácia** - VRRP podporuje MD5(Message Digest 5) algoritmus ako ochranu proti tzv. VRRP - spoofing útoku.

5 Virtuálne privátne siete(VPN)

Z definície je VPN sieť založená medzi zariadeniami, ktoré medzi sebou nezdieľajú žiadnu fyzickú formu pripojenia. Inými slovami je to rozšírenie privátnej siete pomocou nosičov, ktoré predstavujú fyzické infraštruktúry iných sietí. Za najväčší takýto nosič sa dá považovať internet ale môže to byť aj sieť vystavená nejakým poskytovateľom za účelom poskytovania VPN služieb.

VPN je teda súkromné logické spojenie vyhradené autorizovaným osobám pre pripojenie ku vzdialeným zdrojom, pričom na oboch koncoch tohto spojenia sa musí nachádzať patrične nakonfigurovaný hardware/software, ktorý sa stará o procesy súvisiace s tvorbou VPN spojenia(šifrovanie, zapuzdrenie, tunelovanie atď).

Technológií VPN poznáme viacej druhov a to z perspektívy druhej ako aj tretej vrstvy ISO OSI modelu.

Z perspektívy druhej vrstvy:

- Ethernet VLANy
- PVC – Frame Relay alebo ATM
- VPLS

Z perspektívy tretej vrstvy:

- GRE tunely
- IPsec tunely
- MPLS VPN

5.1 Výhody VPN

Jedným z hlavným dôvodov implementácie VPN sietí je zabezpečiť užívateľom, ako sú napríklad zamestnanci firmy, vzdialený a zabezpečený prístup do privátnej siete tejto firmy. Môžeme si predstaviť situáciu, v ktorej prestane fungovať určitá služba, ktorú firma poskytuje svojim zákazníkom a technik, ktorý je za túto službu zodpovedný je buď na dovolenke alebo sa je kvôli inému dôvodu neschopný dostaviť do sídla spoločnosti. V takýchto prípadoch sa hrá o čas a každá minúta kedy je služba nedostupná predstavuje pre spoločnosť finančnú stratu. Aj práve preto je nepraktické aby daný technik strácal čas cestou, ktorý by sa ušetril v prípade, že by bolo možné sa do firemnej siete prihlásiť vzdialene.

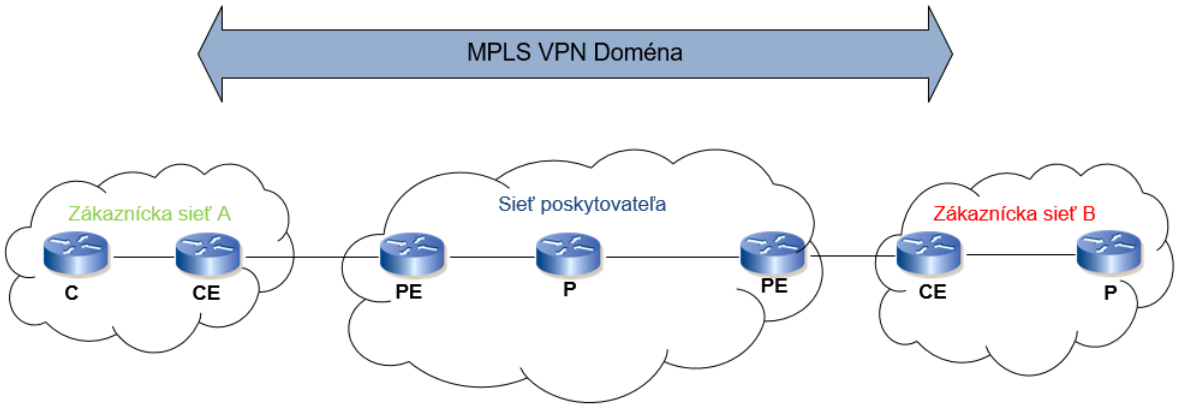
Dôvodov prečo implementovať do sieťovej architektúry VPN je však viac, pričom by som rád vytkol nasledujúce:

- Kontrola – administrátor je schopný jednoducho kontrolovať prístup jednotlivých klientov do firemnej siete.

- Dostupnosť - VPN siete zaručia dostupnosť všetkých zdrojov a sieťových komponentov, ktoré sú dostupné z firemnej siete.
- Zapuzdrenie.
- Rozšíriteľnosť – vo VPN sieťach je možné rozširovať počet klientov podľa potreby.
- Vzdialený prístup – najväčšia výhoda VPN sietí, vďaka ktorej môžu zamestnanci firmy pristupovať do jej sieťovej infraštruktúry z akéhokoľvek miesta, pričom stačí mať internetové pripojenie.

5.2 Multiprotocol label switching VPN

MPLS VPN je rozšírená technológia pri tvorbe VPN sietí popísaná v IETF RFC 4364, ktorá dokáže tieto siete nielen vytvárať ale aj napríklad medzi nimi realizovať spojenie alebo poskytnúť vybranej VPN sieti prístup do internetu. Táto VPN technológia zcela nahradzuje staršie typy technológií využívaných pri tvorbe VPN sietí, ako napríklad Frame-Relay alebo ATM.



Obrázek 6: MPLS VPN topológia

V MPLS VPN sieti je viacero smerovačov, pričom každý zastáva určitú funkciu. Na obrázku 6 je možné vidieť jednotlivé smerovače, ktoré podľa svojho značenia zastávajú následujúce funkcie:

- **P** - Smerovač, ktorý sa nachádza medzi medzi hraničnými smerovačmi MPLS siete a na ktorom je nakonfigurované aktívne MPLS.
- **C** - Smerovač zákazníka, ktorý nemá priame pripojenie do MPLS siete a môže sa preto jednať o zariadenie, ktoré túto technológiu nepodporuje.

- **CE** a **PE** - jedná sa o smerovače, medzi ktorými môže byť implementovaný akýkoľvek smerovací protokol (OSPF, EIGRP..)

Na obrázku 6 je znázornená topológia MPLS VPN siete (peer to peer model), vďaka ktorej je možné prenášať viacero VPN sietí bez nadmerného zaťažovania P smerovača. Toto je docielené vďaka tomu, že každému paketu je priradená určitá značka, vďaka ktorej je možné identifikovať do ktorej VPN siete paket patrí. Tým pádom smerovač nemusí vykonávať zložité smerovacie operácie za účelom zistenia destinácie alebo ďalšieho skoku pre paket a tým pádom nepotrebuje poznať ani adresu destinácie.

Hlavným prvkom v MPLS VPN sieti je PE smerovač, ktorý sa stará o oddeľovanie jednotlivých VPN. Toto delenie je zabezpečené vďaka tomu, že každá VPN pripojená ku tomuto smerovači má svoju vlastnú smerovaciu inštanciu – VRF (Virtual Route Forwarding) a teda vlastnú virtuálnu smerovaciu tabuľku. Každej VPN sieti musí teda náležať práve jedno rozhranie smerovača. Samotné smerovanie vo vnútri MPLS VPN siete je riešené pomocou značiek priradených ku dátovým paketom. Peer to Peer model má v porovnaní s Overlay modelom, využívaným pri Frame Relay alebo ATM niekoľko výhod. Smerovanie v peer to peer modely je jednoduchšie, keďže smerovač si vymieňa smerovacie informácie iba s PE smerovačmi, na ktoré je priamo pripojený.

5.2.1 Základné prvky MPLS VPN sietí

Základné prvky tvoriace VPN siete sa nachádzajú práve na PE smerovači, ktorý je ako už bolo spomenuté vyššie v tejto kapitole, hlavným prvkom MPLS VPN sietí. Tieto prvky sú nasledujúce:

- VRF (Virtual Routing Forwarding)
- RD (Route Distinguisher)
- Route Target

Jednotlivým rozhraniam PE smerovača musí byť pre každú VPN priradená VRF, RD a RT. Vďaka VRF je možné v MPLS VPN sieti vytvoriť jednotlivé VPN. Je to v podstate spojenie smerovacej tabuľky príslušnej VPN a IP smerovacej tabuľky na PE smerovači. Každá VPN sieť tak má vlastnú VRF smerovaciu tabuľku, ktorá je mimo globálnu IP smerovaciu tabuľku. Táto VRF smerovacia tabuľka je vytváraná smerovačom automaticky pre každú VRF inštanciu, pričom má rovnaký tvar ako globálna IP smerovacia tabuľka. Každému rozhraniu PE smerovača môže byť pridelená práve jedna VRF, keďže každému tomuto rozhraniu náleží práve jedna VPN. Pokiaľ chceme konkrétnu VPN pripojiť k viacerým rozhraniam PE smerovača, môžeme týmto rozhraniam priradiť taktiež aj rovnakú VRF.

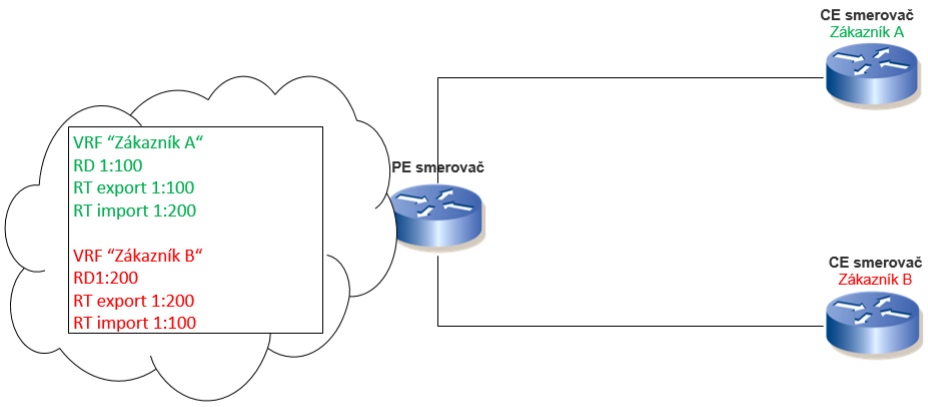
Ku každej VRF je priradený RD, 64 – bitový identifikátor, ktorý spoločne s IPV4 prefixom tvoria VPNv4 prefix. Tento prefix sa ďalej pomocou MP-BGP smerovacieho protokolu prenáša

medzi PE smerovačmi a je vďaka nemu možné využívať pre rôzne VPN siete rovnaké adresné rozsahy. RD identifikátor sa najčastejšie pouzíva vo formáte ASN:nn, pričom ASN predstavuje číslo autonómneho systému a nn je číslo priradené poskytovateľom, a skladá sa z 3 častí:

1. Value field (2 bajty) – určite veľkosť ostávajúcich dvoch polí
2. Administrator Subfield – obsahuje pole ASN
3. Assigned Number Subfield – obsahuje číslo priradené poskytovateľom

Pokiaľ chceme aby bolo možné v rámci MPLS VPN sieti komunikovať medzi jednotlivými VPN sieťami, nestačí použiť len RD identifikátor ale taktiež aj RT identifikátor – Route target. Spojenie, v ktorom medzi sebou komunikujú len smerovače v rámci jednej VPN sa nazýva Intranet a spojenie, v ktorom prebieha komunikácia medzi smerovačmi v rámci rôznych VPN sietí sa nazýva Extranet. Na to aby sme mohli využívať druhého menovaného spojenia je potrebné pridať RT identifikátor, ktorý nám v podstate riadi komunikáciu medzi VPN sieťami. RT sa delí na:

- **Import RT** – Určujú, či sa bude príchodzí VPNv4 prefix vkladať do VRF danej siete. Ak sa hodnota RT zhoduje, sú dáta smerované do danej VRF smerovacej tabuľky, v opačnom prípade sa dáta zahodia.
- **Export RT** – Sú priradené k VPNv4 prefixom prichádzajúcim z konkrétnej VPN siete.



Obrázek 7: Príklad RT importu a RT exportu

5.3 Virtual Route Forwarding(VRF)

VRF je IP technológia, ktorá umožňuje viacerým inštanciám smerovacej tabuľky koexistovať na tom istom smerovači v rovnakom čase. Keďže smerovacie inštancie sú nezávislé, môžeme používať rovnaké IP adresy pre obe inštancie, bez toho aby sme sa obávali duplicitného konfliktu v sieti. Názvom VRF sa taktiež často rozumie virtuálna smerovacia tabuľka, ktorá je v spolupráci s MPLS vyhradená pre konkrétnu VPN sieť. VRF inštancie sú veľa krát spojované práve z MPLS sieťami a ich poskytovateľmi. V takýchto sieťach sa používa MPLS enkapsulácia aby sa izoloval individuálny zákaznícky prevoz a virtuálna smerovacia tabuľka sa udržuje zvlášť pre každého zákazníka. Pre importovanie a exportovanie trás z a do VRF smerovacích tabuliek sa používa najčastejšie MP-BGP smerovací protokol.

Napriek tomu, že vo väčšine prípadov sa VRF používajú hlavne v spolupráci z MPLS, je možné použiť implementáciu VRF aj bez MPLS a v Cisco terminológii sa tejto implementácii hovorí VRF lite.

VRF lite je technológia, ktorá umožňuje poskytovateľovi podporovať dve alebo viac VPN sietí, medzi ktorými je možné prekrývanie IP adries. VRF lite používa vstupné rozhrania na rozlíšenie smerovania pre odlišné VPN siete, pričom priraďuje jeden alebo viac rozhraní tretej vrstvy každej VRF. Tieto rozhrania môžu byť buď fyzické(ethernetový port) alebo logické(virtuálne - SVI) a nemôžu patriť do viac ako práve jednej VRF v daný čas. Aby sa zabezpečil správny presun smerovacích informácií z jednej VRF do druhej je nutné aplikovať medzi týmito VRF export a import smerovacích dráh, keďže pakety, ktoré prichádzajú do konkrétnej VRF, môžu nasledovať smerovacie dráhy len tejto konkrétnej VRF.

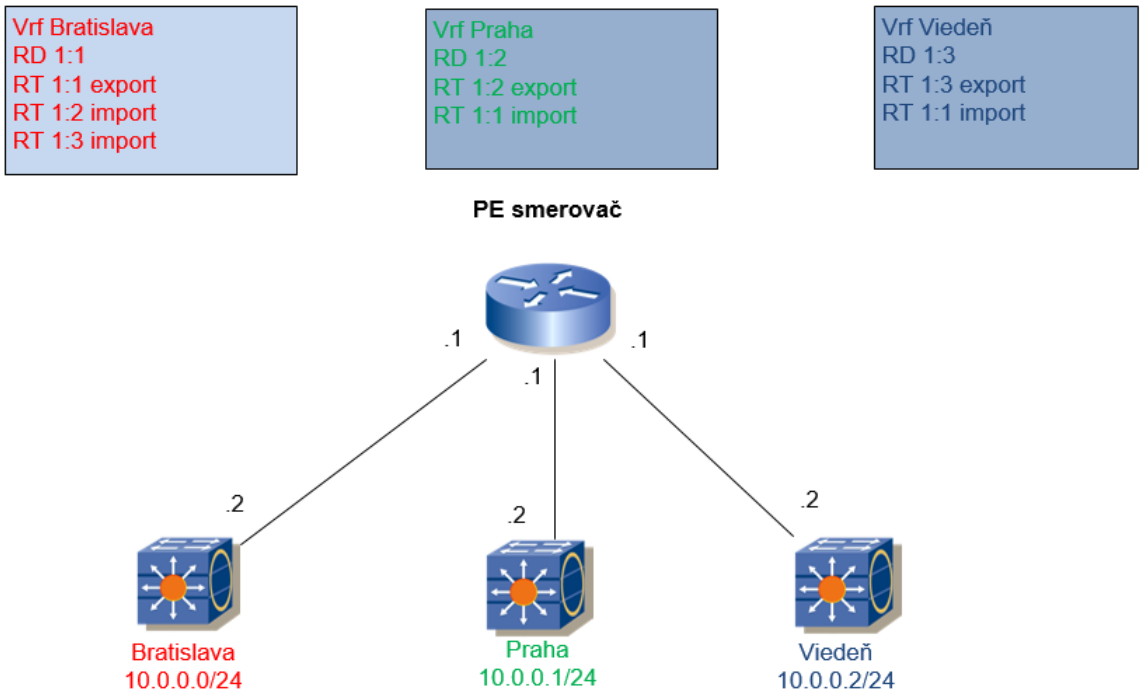
Implementačná schéma VRF lite zahrňuje tieto zariadenia:

- CE (Customer edge) – zariadenia, ktoré poskytujú zákaznícky prístup do siete poskytovateľa, pričom propaguje lokálne smerovacie dráhy do PE smerovača.
- PE (Provider edge) – smerovače, ktoré si vymieňajú smerovacie informácie z CE zariadeniami za použitia statického smerovania, alebo smerovacích protokolov (OSPF, BGP atď.)
- Smerovače poskytovateľa – akýkoľvek smerovač v sieti poskytovateľa, ktorý nie je priamo pripojený k CE zariadeniu.

PE smerovač je zodpovedný za udržiavanie smerovacích trás len tých VPN, ktoré sú ku nemu priamo priradené a nemusí sa tak starať o smerovacie informácie všetkých VPN poskytovateľa.

V konkrétnom riešení u poskytovateľa, každý PE smerovač udržiava VRF pre každú z priamo pripojených zákazníckych pobočiek. Viaceré rozhrania smerovača môžu byť priradené jednej VRF v prípade, že viacej zákazníckych pobočiek zdieľa rovnakú VPN, pričom každá VPN je mapovaná pre špecifickú VRF. Potom čo sa PE smerovač naučí lokálne VPN smerovacie informácie, začne zdieľať VPN smerovacie informácie s inými PE smerovačmi za použitia interného BGP(IBGP).

S VRF lite môže viacero zákazníkov zdieľať jedno CE zariadenie, pričom je použitá len jedna fyzická linka medzi CE a PE smerovačom. Toto zdieľané CE udržiava separátne VRF smerovacie tabuľky pre každého zákazníka a prepína alebo smeruje pakety na základe toho o akého zákazníka sa jedná a akú VRF smerovaciu tabuľku má priradenú. VRF lite taktiež rozširuje funkcionalitu PE smerovača na CE zariadenie, čo mu umožňuje udržiavať separátne VRF smerovacie tabuľky pre zlepšenie súkromia a bezpečnosti VPN siete zákazníckej pobočky.

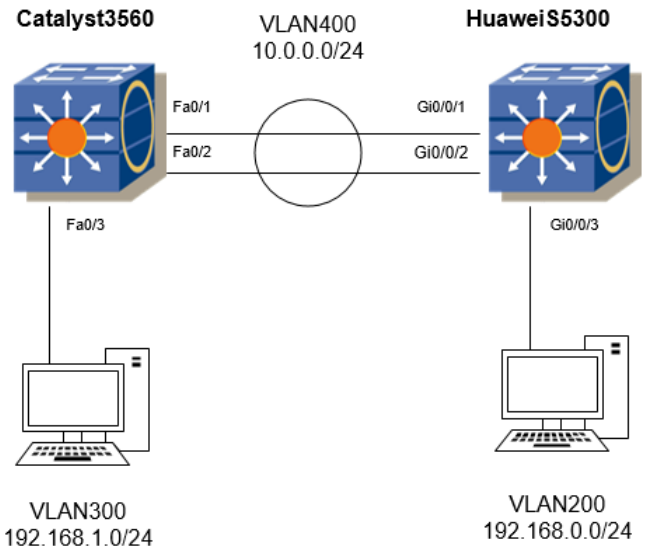


Obrázek 8: Príklad VRF lite konfigurácie

Na obrázku 8 je predvedený príklad VRF lite konfigurácie. V sieťach označených ako Bratislava, Praha a Viedeň je ako smerovací protokol použité OSPF. Pre každú z týchto sietí beží nezávisle OSPF proces, ktorý naplní smerovaciu tabuľku ich príslušnej VRF. Následne je za pomoci smerovacieho protokolu BGP a RT importu a exportu možno ovplyvňovať medzi ktorými VRF budeme vymieňať smerovacie informácie. Pri tomto konkrétnom nastavení je umožnená komunikácia medzi sieťami Bratislava - Praha a Bratislava - Viedeň, pretože si vymieňajú svoje smerovacie informácie. Komunikácia medzi sieťami Praha a Viedeň však možná nieje, pretože si svoje smerovacie informácie nevymieňajú a teda o sebe nevedia.

6 Konfigurácia technológií EtherChannel, SVI a InterVLAN routing

Pred začatím samotnej konfigurácie bolo nutné vytvoriť topológiu siete v ktorej by bolo možné technológie EtherChannel, SVI a InterVLAN routing použiť. Pre konfiguráciu týchto technológií mi stačilo navrhnúť jednoduchú topológiu, ktorá pozostávala z dvoch prepínačoch, prepojených dvomi UTP káblami pre vytvorenie EtherChannelu, pričom do každého z prepínačov bolo pripojené koncové zariadenie reprezentujúce konkrétnu VLAN sieť. Keďže v tejto práci testujem spoluprácu platforiem Cisco a Huawei, použité prepínače boli konkrétne Cisco Catalyst 3560 a Huawei S5300.



Obrázek 9: Schéma zapojenia pre konfiguráciu InterVLAN routing, SVI a EtherChannel

Na schéme zapojenia, ktorú je možné vidieť na obrázku 9, sú znázornené tri VLAN siete. VLAN 200 a VLAN 300 slúžia pre užívateľské siete a VLAN400 je určená pre smerovanie medzi týmito dvoma sieťami. Na každom z prepínačov boli vytvorené dve SVI rozhrania, jedno pre príslušnú užívateľskú VLAN sieť, ktoré pre danú sieť slúžilo ako východzia brána a druhé pre "smerovaciu"VLAN sieť.

6.1 Konfigurácia prepínača Cisco Catalyst 3560

Na začiatku bolo nutné vytvoriť potrebné VLAN siete, dve užívateľské a jednu pre smerovanie. Je dobré spomenúť, že operačný systém bežiaci na Cisco prepínači nám po nabootovaní umožnil okamžite konfigurovať a od užívateľa neboli potrebné žiadne ďalšie nastavenia. Pre prechod do konfiguračného režimu je potrebné sa dostať najprv do enable režimu príkazom `enable` a v tomto režime zadať príkaz `configure terminal`

```
Switch# configure terminal
Switch(config)# vlan 300
Switch(config-vlan)# name 300

Switch(config)# vlan 400
Switch(config-vlan)# name 400

Switch(config)# vlan 200
Switch(config-vlan)# name 200
```

Následne bolo potrebná nastaviť jednotlivé rozhrania na prepínači vrátane virtuálneho Port-channelu a priradiť im príslušné VLAN siete. Fyzické rozhrania `FastEthernet0/1` a `FastEthernet0/2` bolo nutné priradiť do virtuálneho port-channelu a zvoliť LACP mód active. Pri konfigurácii rozhraní na prepínačoch Cisco sa taktiež vyberá enkapsulačný protokol, ktorý sa nastavuje na trunk rozhraniach a je potrebný pre prepínač aby vedel rozoznávať rámce z jednotlivých VLAN sietí. V našom prípade bol použitý protokol 802.1Q.

```
Switch(config)#interface Port-channel 1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 200,300,400

Switch(config)#interface FastEthernet0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 200,300,400
Switch(config-if)#channel-group 1 mode active

Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 200,300,400
Switch(config-if)#channel-group 1 mode active
```

```
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 300
```

V poslednom kroku bolo potrebné vytvoriť dve SVI rozhrania a zabezpečiť smerovanie pre dáta z VLAN siete 400. Jedno SVI rozhranie nám slúži ako východzia brána pre VLAN sieť 300 a druhé pre smerovanie dát. Na Cisco prepínači Catalyst 3560 bolo nutné zabezpečiť L3 funkcionalitu príkazom `ip routing`.

```
Switch(config)#interface Vlan300
Switch(config-if)#ip address 192.168.1.1 255.255.255.0

Switch(config)#interface Vlan400
Switch(config-if)#ip address 10.0.0.1 255.255.255.0

ip route 192.168.0.0 255.255.255.0 10.0.0.2
```

6.2 Konfigurácia prepínača Huawei S5300

Pred zahájením samotnej konfigurácie na prepínači Huawei S5300 je užívateľ vyzvaný k nastavení systémového hesla, ktoré bude slúžiť pre autentifikáciu pri ďalších prihláseniach do konzoly.

Po nastavení hesla bolo nutné prejsť do konfiguračného režimu, na čo slúži príkaz `system-view`. Obdobne ako u Cisco prepínača, začiatok konfigurácie spočíval vo vytvorení VLAN sietí.

```
[Huawei] vlan 200
[Huawei-vlan200] name 200
[Huawei-vlan200] quit

[Huawei] vlan 300
[Huawei-vlan300] name 300
[Huawei-vlan300] quit

[Huawei] vlan 400
[Huawei-vlan400] name 400
[Huawei-vlan400] quit
```

Následne bolo potrebné nastaviť jednotlivé rozhrania. V porovnaní s Cisco prepínačom bola táto konfigurácia kratšia a jednoduchšia, nakoľko stačilo nakonfigurovať len virtuálne rozhranie Eth-Trunk a fyzické potom už len ku tomuto virtuálnemu rozhraniu priradiť. Konfigurácia

virtuálneho rozhrania spočívala vo zvolení typu rozhrania - trunk, vo výbere protokolu LACP, ktorý je u Huawei prepínačov automaticky v móde active (ak ho užívateľ nenastaví inak), a ku priradení VLAN sietí tomuto rozhraniu. U Huawei prepínača nebolo nutné voliť v Eth-Trunk rozhraní enkapsulačný protokol, keďže sa automaticky používa 802.1Q.

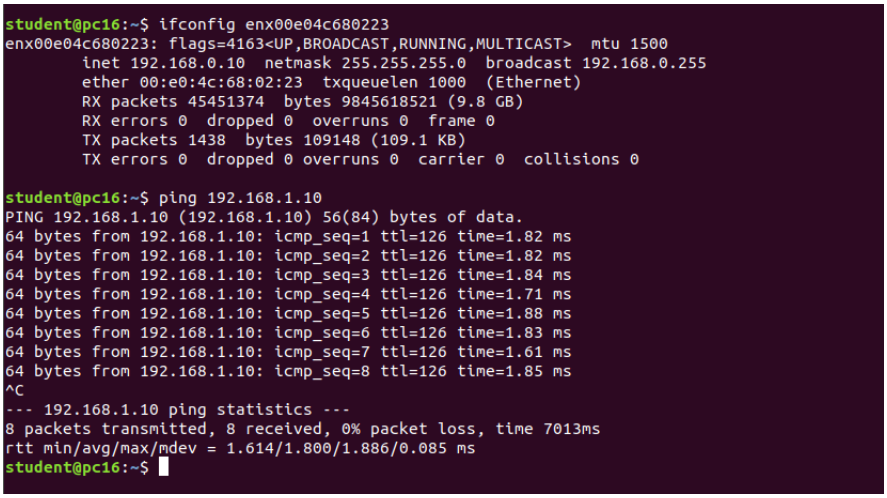
```
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] port link-type trunk
[HUAWEI-Eth-Trunk1] port trunk allow-pass vlan 200 300 400
[HUAWEI-Eth-Trunk1] mode lacp

[HUAWEI] interface GigabitEthernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 1

[HUAWEI] interface GigabitEthernet0/0/2
[HUAWEI-GigabitEthernet0/0/2] eth-trunk 1
```

Na záver zostávalo už len vytvorenie SVI rozhraní a zabezpečenie smerovania medzi VLAN sieťami. U Huawei prepínača oproti Cisco prepínaču nebolo nutné zvlášť zapínať L3 funkcionalitu.

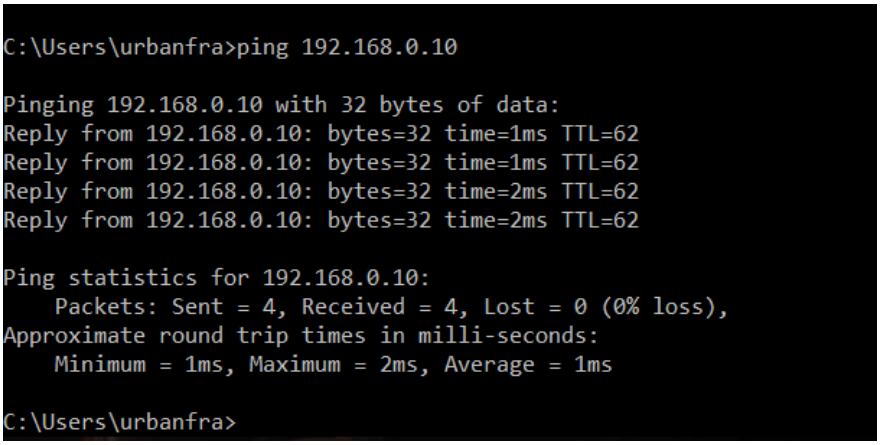
```
[HUAWEI] interface vlanif 200
[HUAWEI-Vlanif200] ip address 192.168.0.1 255.255.255.0

[HUAWEI] interface vlanif 400
[HUAWEI-Vlanif400] ip address 10.0.0.2 255.255.255.0

[HUAWEI] ip route-static 192.168.1.0 255.255.255.0 10.0.0.1
```

6.3 Testovanie funkcionality

Pre overenie funkcionality InterVLAN smerovania boli použité dve užívateľské stanice, každá reprezentujúca jednu VLAN sieť. Na užívateľskej stanici VLAN 300 bol použitý operačný systém Windows 10, na sieťovom rozhraní Ethernet bola nastavená IP adresa `192.168.1.10` a ako východzia brána bolo použité SVI rozhranie na prepínači Cisco Catalyst 3560. Užívateľská stanica reprezentujúca VLAN 200 používala operačný systém Ubuntu, jej Ethernet rozhranie malo nakonfigurovanú IP adresu `192.168.0.10` a ako východzia brána bolo použité SVI rozhranie na prepínači Huawei S5300. Pre overenie konektivity bol použitý príkaz `ping`.



Obrázek 10: Úspešný `ping` z užívateľskej stanice VLAN200 na stanicu VLAN300



Obrázek 11: Úspešný `ping` z užívateľskej stanice VLAN300 na stanicu VLAN200

Správna funkcionalita technológie EtherChannel bola overená príkazmi `show` na prepínači Cisco Catalyst 3560 a `display` na prepínači Huawei S5300.

```
Switch#show interfaces port-channel 1 etherchannel
Port-channel1   (Primary aggregator)

Age of the Port-channel   = 0d:00h:44m:58s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             0
  0     00     Fa0/2    Active             0

Time since last port bundled:    0d:00h:36m:27s    Fa0/2
```

Obrázek 12: Výstup z príkazu `show interfaces` na Cisco prepínači

Na obrázku 12 je možné vidieť zobrazenie virtuálneho port-channel rozhrania na Cisco prepínači, ktoré obsahuje viacero užitočných informácií ako napríklad zoznam fyzických portov, čas kedy sa port-channel naviazal alebo použitý protokol (štandardizovaný LACP alebo Cisco proprietárny PAgP), v našom prípade LACP. Oproti Cisco prepínači, výpisok eth-trunk virtuálneho rozhrania na Huawei prepínači, ktorý je možné vidieť na obrázku 14, neobsahuje informáciu o použitom protokole, pretože používa len štandardizovaný LACP protokol. Výpisok na Huawei prepínači však obsahuje niekoľko dodatočných užitočných informácii, ako napríklad vstupné a výstupné vyťaženie eth-trunk rozhrania alebo aktuálna šírka pásma. Aj napriek tomu, že na Huawei prepínači boli použité pre virtuálne trunk rozhranie dve fyzické Gigabit Ethernet rozhrania, je možné vo výpisku vidieť hodnotu BW(šírka pásma) len 200 Mbit/s. Je to kvôli tomu, že na protiľahlom Cisco prepínači boli pre virtuálny port-channel použité dve Fast Ethernet rozhrania, každé s prenosovou rýchlosťou 100Mbit/s.

```
Switch#show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Fa0/1     SA      bndl      32768         0x1       0x1     0x104       0x3D
Fa0/2     SA      bndl      32768         0x1       0x1     0x105       0x3D
Switch#
```

Obrázek 13: Výstup z príkazu `show lacp` na Cisco prepínači

Na obrázku 13 je možné vidieť výpisok z LACP protokolu, ktorý obsahuje informácie ako mód v akom LACP protokol pracuje alebo prioritu jednotlivých fyzických portov, na základe

ktorej sa určite, ktoré porty budú v port-channel skupine aktívne. Pred samotným výpiskom je zoznam značiek označených ako "Flags", pomocou ktorých vie užívateľ určiť v akom móde rozhrania pracujú. V našom prípade značka SA znamená, že si zariadenie aktívne(LACP je v active móde) vyžaduje pomalé LACPDU dátové jednotky. Na obrázku 15 je zobrazený výpis LACP štatistík, ktorý umožňoval Huawei prepínač. Užívateľ tu môže vidieť informácie o počte odoslaných a prijatých LACPDU dátových jednotiek na jednotlivých fyzických rozhraniach.

```
[Quidway]display interface Eth-Trunk 1
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:HUAWEI, Quidway Series, Eth-Trunk1 Interface
Switch Port, PVID :    1, Hash arithmetic : According to SA-XOR-DA,Maximal BW: 200M, Current BW: 200M, The Maximum Frame Length is 2044
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 781d-bad4-711a
    Input bandwidth utilization  : 0.01%
    Output bandwidth utilization : 0.01%
--------------------------------------------------
PortName                      Status      Weight
--------------------------------------------------
Ethernet0/0/1                 UP          1
Ethernet0/0/2                 UP          1
--------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
```

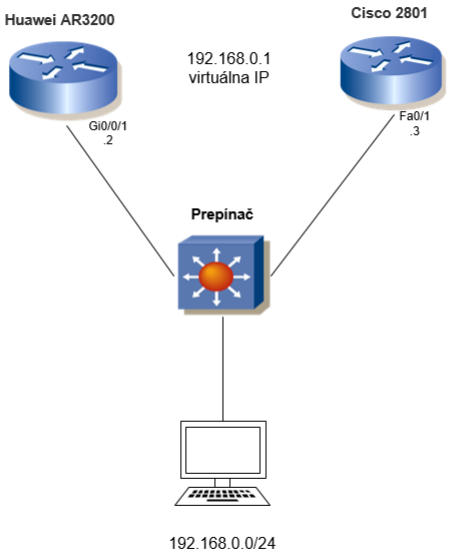
Obrázek 14: Výstup z príkazu `display interface` na Huawei prepínači

```
[Quidway]display lacp statistics eth-trunk 1
 Eth-Trunk1's PDU statistic is:
 --------------------------------------------------------------------------------
 Port                      LacpRevPdu   LacpSentPdu  MarkerRevPdu MarkerSentPdu
 Ethernet0/0/1             78           257          0            0
 Ethernet0/0/2             80           706          0            0
```

Obrázek 15: Výstup z príkazu `display lacp statistics` na Huawei prepínači

7 Konfigurácie technológie VRRP

Schéma zapojenia pre testovanie VRRP pozostávala z dvoch smerovačoch, prepínača a testovacej stanice. Ako Cisco smerovač bol použitý Cisco 2801 Integrated Services Router a Huawei platformu v tomto zapojení zastával Huawei AR3200. Testovacia stanica náležala sieti **192.168.0.0/24** a ako východzia brána pre hosťovské adresy tejto siete bola použitá virtuálna VRRP IP adresa **192.168.0.1**. Fyzickým rozhraniam oboch smerovačoch boli priradené IP adresy **192.168.0.2** pre Huawei smerovač, ktorý v tomto zapojení zastával úlohu "Master"a **192.168.0.3** pre Cisco smerovač, ktorý zastával úlohu "Backup". Schéma zapojenia je znázornená na obrázku 16.



Obrázek 16: Schéma zapojenia pre konfiguráciu VRRP

7.1 Konfigurácia smerovača Cisco 2801 Integrated Services Router

Obdobne ako pri konfigurácii Cisco prepínača tak ani u Cisco smerovača neboli potrebné žiadne úvodné nastavenia a po nabootovaní systému stačilo prejsť príkazom `enable` do enable režimu a následne príkazom `configure terminal` do konfiguračného režimu. pre konfiguráciu technológie VRRP stačilo nakonfigurovať len jedno fyzické rozhranie, ktorému bolo nutné prideliť príslušnú IP adresu a masku a následne ho prideliť do vrrp skupiny a definovať virtuálnu VRRP IP adresu.

```
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.0.3 255.255.255.0
Router(config-if)#vrrp 1 ip 192.168.0.1
Router(config-if)#vrrp 1 timers learn
Router(config-if)#vrrp 1 priority 90
```

Pri tejto konkrétnej konfigurácii bola rozhraniu Cisco smerovača pridelená VRRP priorita 90, čím sa docielilo, že Cisco smerovač prevzal úlohu "Backup". Príkazom `timers learn` bolo docielené aby sa smerovač učil VRRP advertising časové intervaly smerovača, ktorý je v role master. Vo VRRP skupine je potrebné aby boli na všetkých smerovačoch nastavené rovnaké časové intervaly inak by dochádzalo ku chybám v komunikácii medzi jednotlivými smerovačmi na ktorých by sa tieto časové intervaly nezhodovali.

7.2 Konfigurácia smerovača Huawei AR3200

Pri konfigurácii Huawei smerovača, obdobne ako pri konfigurácii Huawei prepínača je pred začatím samotnej konfigurácie užívateľ vyzvaný k nastavení systémového hesla, ktoré bude slúžiť pre autentifikáciu pri ďalších prihláseniach do konzoly.

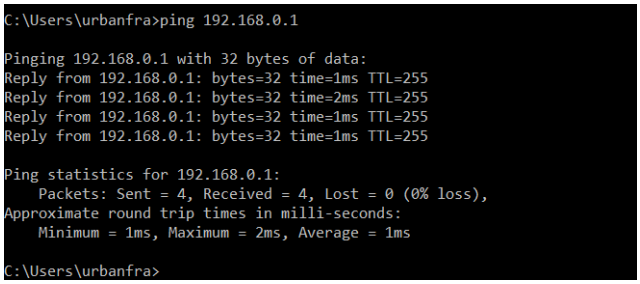
Po prechode do konfiguračného režimu príkazom `system-view` stačilo obdobne ako u Cisco smerovača nakonfigurovať len jedno fyzické rozhranie, ktorému bola priradená IP adresa, maska a virtuálna VRRP IP adresa.

```
[HUAWEI] interface GigabitEthernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.0.2 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 192.168.0.1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 priority 120
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 timer advertise 2
```

Huawei smerovač bol v tejto konfigurácii určený ako "Master"nastavením vyššej priority, v našom prípade 120. Časový interval v ktorom sa budú posielať VRRP advertising správy bol nastavený na 2 sekundy. Ak smerovač v úlohe "Backup"neobdrží VRRP správu od master smerovača po dobu tri krát dlhšiu ako nastavený časový interval tak prevezme jeho rolu a prejde do role "Master". Je dobré spomenúť, že u Huawei smerovača bolo možné použiť VRRP verziu 3, prednastavená verzia je verzia 2, ktorá bola pri konfigurácii použitá keďže Cisco prepínač verziu 3 nepodporoval.

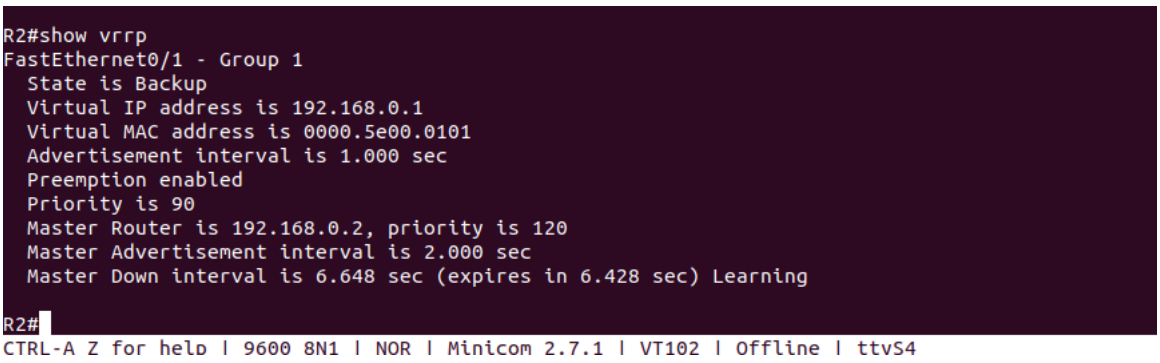
7.3 Testovanie funkcionality VRRP

Pre overenie funkcionality VRRP bola použitá užívateľská stanica s operačným systémom Windows 10, ktorej bola priradená adresa `192.168.0.10` z príslušného rozsahu. Funkcionalita bola overená príkazom `ping` na východziu bránu, ktorou bola nakonfigurovaná virtuálna VRRP IP adresa.



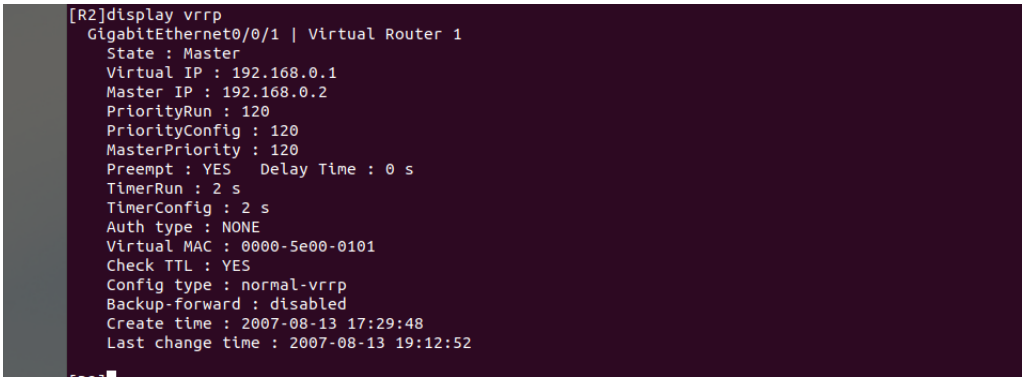
Obrázek 17: Úspešný `ping` z užívateľskej stanice na virtuálnu VRRP adresu

Správna funkcionalita technológie VRRP bola taktiež overená príkazmi `show` na smerovači Cisco a `display` na smerovači Huawei.



Obrázek 18: Výstup z príkazu `show vrrp` na Cisco smerovači

Na obrázku 18 je možné vidieť informácie o VRRP protokole na Cisco smerovači, ako napríklad fyzické rozhranie a jeho priradenie ku danej VRRP skupine, stav v akom sa rozhranie nachádza("master"alebo "backup"), jeho prioritu, virtuálna IP adresa pre danú VRRP skupinu alebo IP adresu rozhrania, ktoré je v danej skupine označené ako "master". S výpisku je možné vidieť, že priorita rozhrania na Cisco smerovači bola nastavená na hodnotu 90 a nachádza sa v stave "backup", pričom ako "master"bolo zvolené rozhranie na Huawei smerovači s IP adresou 192.168.0.2 s prioritou 120. Výpisok VRRP protokolu na Huawei smerovači, ktorý je možné vidieť na obrázku 19, obsahuje obdobné informácie ako výpisok na Cisco smerovači, avšak neobsahuje informácie o rozhraní, ktoré je v stave "backup".

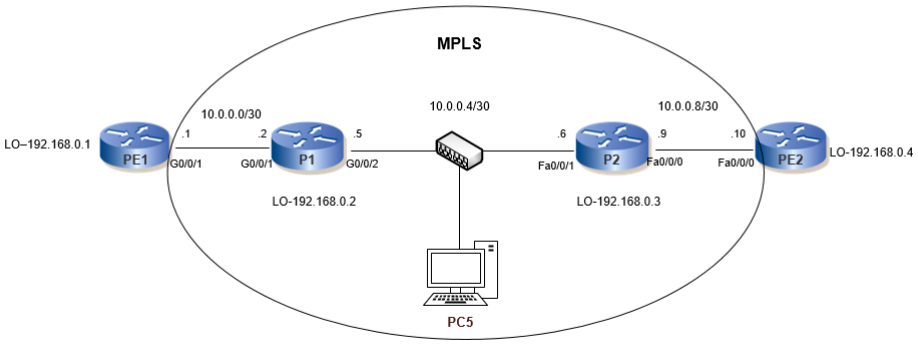


Obrázek 19: Výstup z príkazu `display vrrp` na Huawei smerovači

8 Konfigurácia technológie MPLS VPN

Pred začiatkom samotnej konfigurácie bolo nutné navrhnúť vhodnú topológiu, ktorá by bola realizovateľná z hľadiska dostupných prostriedkov a kapacity, a ktorá by zároveň spĺňala hlavné prvky a funkcionalitu MPLS VPN siete. Taktiež bolo nutné topológiu navrhnúť tak aby bola jednoznačne preukázateľná vzájomná spolupráca platforiem Cisco a Huawei.

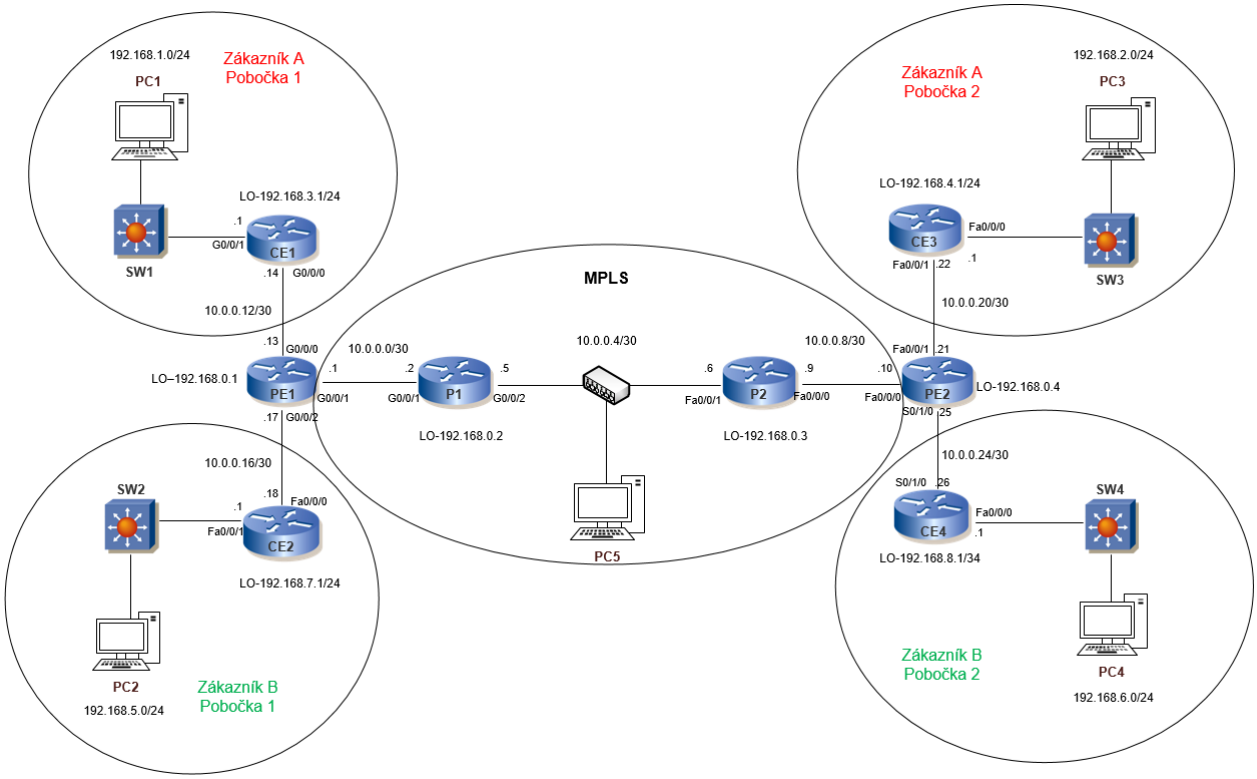
S ohľadom na všetky tieto faktory, pozostávala sieť poskytovateľa zo štyroch smerovačov značených ako PE1,PE2,P1 a P2. Ako prvý hraničný smerovač poskytovateľa(PE1)bol použitý smerovač Huawei AR3200 a ako druhý hraničný smerovač poskytovateľa(PE2)bol použitý smerovač Cisco2801s. Vnútro siete poskytovateľa tvorili smerovače Huawei AR2200(P1) a Cisco2801s(P2). Medzi týmito štyrmi smerovačmi bola implementovaná technológia MPLS a ako interný smerovací protokol bolo použité OSPF. Každý smerovač mal nakonfigurovanú adresu rozhrania loopback, ktorá slúžila pre jeho LSR(Label Switching Router) identifikáciu v MPLS sieti. Medzi smerovačmi P1 a P2 bola zapojená užívateľská stanica pomocou HUB zariadenia, ktorá slúžila pre overenie funkcionality v programe Wireshark. Topológia MPLS siete poskytovateľa je znázornená na obrázku 20.



Obrázek 20: Topológia MPLS siete poskytovateľa

Pre aplikovanie technológie MPLS VPN bolo nutné navrhnúť do topológie zákaznícke siete, ktoré by využívali stávajúcu MPLS sieť poskytovateľa. Aby sa demonštrovali faktory správnej funkcionality VPN siete, akým je napríklad oddelenie IP prevádzky rôznych zákazníkov, bola topológia rozšírená o dve zákaznícke siete, pričom každej zákazníckej sieti náležali dve pobočky. Pre rozšírenie topológie boli použité ďalšie štyri smerovače značené ako CE1-4 a štyri prepínače značené ako SW1-4. Ako prvý hraničný smerovač zákazníckej siete(CE1)bol použitý Huawei AR1220, pre zvyšné tri zákaznícke hraničné smerovače bol použitý Cisco2600s. Každej pobočke náležala užívateľská stanica, z ktorej bola testovaná komunikácia na protiľahlú pobočku daného zákazníka.

Zákazníkovi A boli priradené štyri IP prefixy, dva pre každú jeho pobočku, pričom prvej pobočke náležali prefixy 192.168.1.0/24 a 192.168.3.0/24 a druhej pobočke prefixy 192.168.2.0/24 a 192.168.4.0/24. Obdobne to bolo aj u zákazníka B, ktorého prvej pobočke boli priradené prefixy 192.168.5.0/24 a 192.168.7.0/24 a druhej pobočke prefixy 192.168.6.0 a 192.168.8.0/24. Jedna zo sietí na každej pobočke bola simulovaná rozhraním loopback. Kompletnú topológiu technológie MPLS VPN je môžné vidieť na obrázku



Obrázek 21: Kompletná topológia MPLS VPN siete

8.1 Konfigurácia MPLS siete poskytovateľa

V prvom kroku implementácie MPLS VPN technológie bolo nutné správne nastaviť MPLS v sieti poskytovateľa. Ako interný smerovací protokol bolo použité OSPF, pričom IP prefixy určené na prepojenia medzi jednotlivými smerovačmi sú znázornené na obrázkoch 21 a 20.

8.1.1 Konfigurácia smerovača PE1

Konfigurácia smerovača Huawei AR3200 v pozícii hraničného smerovača poskytovateľa PE1 pozostávala z niekoľkých krokov. Na začiatku bolo nutné nastaviť jednotlivé rozhrania priradením ich príslušných IP adries. Rozhranie loopback v tomto prípade slúži pre LSR identifikáciu smerovača v MPLS sieti.

```
[PE1] interface GigabitEthernet0/0/1
```

```
[PE1-GigabitEthernet0/0/1] ip address 10.0.0.1 255.255.255.252
[PE1-GigabitEthernet0/0/1] description PE1->P1

[PE1] interface lo0
[PE1-LoopBack0] ip address 192.168.0.1 255.255.255.255
```

Následná konfigurácia OSPF pozostávala z označenia smerovacieho procesu(v našom prípade som proces pre interné smerovacie potreby označil číslom 1), priradeniu prefixov ktoré chceme smerovač a výber smerovacej oblasti.

```
[PE1]ospf 1
[PE1-ospf-1]area 0
[PE1-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.3
[PE1-ospf-1-area-0.0.0.0]network 192.168.0.1 0.0.0.0
```

Po nakonfigurovaní rozhraní a OSPF procesu nasledovala konfigurácia samotného MPLS. Na Huawei smerovačoch je nutné zapnúť MPLS globálne a na to aby sme MPLS mohli spustiť globálne je nutní smerovaču prideliť jeho LSR identifikáciu, v našom prípade nám pre tento účel poslúžila adresa rozhrania loopback 0.

```
[PE1]mpls lsr-id 192.168.0.1
[PE1]mpls
```

Globálne bolo taktiež nutné v sekcii mpls zapnúť zasielanie MPLS značiek, bez ktorého by sa k IP prefixom nepriraďovali MPLS značky, a rovnako bolo nutné povoliť protokol LDP, ktorý slúži na výmenu MPLS značiek medzi LSR smerovačmi.

```
[PE1-mpls]lsp-trigger all
[PE1]mpls ldp
```

Následne už len ostávalo zapnúť MPLS a ldp explicitne na potrebných rozhraniach.

```
[PE1] interface GigabitEthernet0/0/1
[PE1-GigabitEthernet0/0/1]mpls
[PE1-GigabitEthernet0/0/1]mpls ldp
```

Funkcionalitu MPLS je na Huawei smerovačoch možné overiť príkazom `display mpls lsp`, ktorý zobrazí LFIB databázu.

8.1.2 Konfigurácia smerovača PE2

Konfigurácia smerovača Cisco 2600s vo funkcii smerovača PE2 sa od konfigurácie na smerovači Huawei moc nelíšila. V prvom rade bolo nutné na Cisco smerovači zapnúť CEF(Cisco Express Forwarding), čo je Cisco proprietárna rozšírená L3 prepínacia technológia, často používaná vo veľkých sieťach poskytovateľa. Po nastavení rozhraní a OSPF bolo nutné globálne povoliť signalizačný protokol LDP a zabezpečiť naviazanie LDP väzby z rozhrania loopback. Na záver bolo obdobne ako na Huawei smerovači nutné povoliť MPLS explicitne na potrebných rozhraniach.

```
PE2(config)#ip cef

PE2(config)#interface FastEthernet0/0
PE2(config-if)#ip address 10.0.0.10 255.255.255.252
PE2(config-if)#description PE2->P2
PE2(config-if)#no shut

PE2(config)#interface Loopback0
PE2(config-if)#ip address 192.168.0.4 255.255.255.255
PE2(config-if)#no shut

PE2(config)#router ospf 1
PE2(config-router)#network 10.0.0.8 0.0.0.3 area 0
PE2(config-router)#network 192.168.0.4 0.0.0.0 area 0

PE2(config)#mpls label protocol ldp
PE2(config)#mpls ldp router-id Loopback0 force

PE2(config)#interface FastEthernet0/0
PE2(config-if)#mpls ip
```

Výpis konfigurácie zo všetkých LSR smerovačov je možné nájsť v prílohe.

8.2 Konfigurácia technológie MPLS VPN na hraničných smerovačoch poskytovateľa

Po zabezpečení funkcionality MPLS vo vnútornej sieti poskytovateľa bolo nutné správne nakonfigurovať hraničné smerovače poskytovateľa PE1 a PE2. Každý z týchto smerovačov zastával funkciu prístupového bodu do siete poskytovateľa pre dve zákaznícke pobočky, pričom každej pobočke náležali dva IP prefixy. Pre výmenu prefixov medzi pobočkami daného zákazníka bol použitý smerovací protokol MP BGP, teda medzi oboma hraničnými smerovačmi poskytovateľa musela byť vytvorená BGP väzba.

8.2.1 Konfigurácia smerovača PE1

V prvom kroku bolo nutné pre každého zákazníka vytvoriť vrf smerovaciu inštanciu. Každej vrf inštancii bol priradený RD (Route distinguisher), vďaka ktorému je možné v sieti oddeliť jednotlivé prefixy medzi rôznymi zákazníkmi, a RT (Route target), ktorý definuje z ktorých inštancií chceme prijímať smerovacie informacie a naopak do ktorých inštancií chceme smerovacie informácie odosielať.

```
[PE1]ip vpn-instance Zakaznik_A
[PE1-vpn-instance-Zakaznik_A]ipv4-family
[PE1-vpn-instance-Zakaznik_A]route-distinguisher 1:100
[PE1-vpn-instance-Zakaznik_A]vpn-target 1:100 export-extcommunity
[PE1-vpn-instance-Zakaznik_A]vpn-target 1:100 import-extcommunity

[PE1]ip vpn-instance Zakaznik_B
[PE1-vpn-instance-Zakaznik_B]ipv4-family
[PE1-vpn-instance-Zakaznik_B]route-distinguisher 1:200
[PE1-vpn-instance-Zakaznik_B]vpn-target 1:200 export-extcommunity
[PE1-vpn-instance-Zakaznik_B]vpn-target 1:200 import-extcommunity
```

Po vytvorení zákazníckych vrf inštancií, bolo potrebné tieto inštancie priradiť fyzickým rozhraniam hraničného smerovača ku ktorým sú pripojené jednotlivé zákaznícke pobočky. Na Huawei smerovači sa po priradený vrf inštancie fyzickému rozhraniu premaže jeho IP konfigurácie, preto je vhodné IP konfigurovať až po priradený vrf inštancie.

```
[PE1]interface GigabitEthernet0/0/0
[PE1-GigabitEthernet0/0/0]ip binding vpn-instance Zakaznik_A
[PE1-GigabitEthernet0/0/0]ip address 10.0.0.13 255.255.255.252
[PE1-GigabitEthernet0/0/0]description PE1-CE1

[PE1]interface GigabitEthernet0/0/2
[PE1-GigabitEthernet0/0/2]ip binding vpn-instance Zakaznik_B
[PE1-GigabitEthernet0/0/2]ip address 10.0.0.17 255.255.255.252
[PE1-GigabitEthernet0/0/2]description PE1-CE2
```

Ďalší krok pozostával z konfigurácie OSPF procesov pre každého zákazníka. OSPF proces 1 bol použitý pre interné smerovanie v sieti poskytovateľa, zákazníkovi A bol priradený OSPF proces 2 a zákazníkovi B bol priradený OSPF proces 3.

```
[PE1]ospf 2 vpn-instance Zakaznik_A
[PE1-ospf-2]area 0.0.0.0
[PE1-ospf-2-area-0.0.0.0]network 10.0.0.12 0.0.0.3

[PE1]ospf 3 vpn-instance Zakaznik_B
[PE1-ospf-3]area 0.0.0.0
[PE1-ospf-3-area-0.0.0.0]network 10.0.0.16 0.0.0.3
```

Pre naviazanie BGP väzby s protiľahlým hraničným smerovačom PE2 poslúžili adresy rozhraní Loopback0. Keďže bolo pre označenie RD použité prvé číslo 1, použilo sa rovnaké číslo aj pre značenie BGP autonómneho systému. Kvôli použitiu MP-BGP nebolo nutné používať špecifikáciu rodiny adries ku BGP susedovi a mohli sme ju teda vypnúť.

```
[PE1]bgp 1
[PE1-bgp]peer 192.168.0.4 as-number 1
[PE1-bgp]peer 192.168.0.4 connect-interface LoopBack0
[PE1-bgp]ipv4-family unicast
[PE1-bgp-af-ipv4] undo synchronization
[PE1-bgp-af-ipv4] undo peer 192.168.0.4 enable
```

Ďalší krok pozostával z konfigurácie rodiny adries VPNv4, kde bolo nutné pre BGP väzbu aktivovať zasielanie VPNv4 prefixov a vnútorných značiek, rovnako ako aj výmenu RT značiek, na čo slúžil príkaz `policy vpn-target`.

```
[PE1-bgp]ipv4-family vpnv4
[PE1-bgp-af-vpnv4]policy vpn-target
[PE1-bgp-af-vpnv4]peer 192.168.0.4 enable
```

Aby sme mohli redistribuovať prefixy naučené pomocou OSPF z jedného hraničného smerovača na druhý pomocou protokolu BGP, je nutné spraviť redistribúciu z oboch OSPF procesov zákazníka do MP-BGP. Príkaz `import-route direct` v tom prípade slúžil pre redistribúciu podsietí medzi PE1-CE1 u zákazníka A a PE1-CE2 u zákazníka B.

```
[PE1-bgp]ipv4-family vpn-instance Zakaznik_A
[PE1-bgp-Zakaznik_A]import-route direct
[PE1-bgp-Zakaznik_A]import-route ospf 2

[PE1-bgp]ipv4-family vpn-instance Zakaznik_B
[PE1-bgp-Zakaznik_B]import-route direct
[PE1-bgp-Zakaznik_B]import-route ospf 3
```

Redistribúciu je potrebné taktiež zapnúť aj opačne z BGP do OSPF aby zákazníci dostávali vzdialené IP prefixy v OSPF aktualizáciách.

```
[PE1]ospf 2 vpn-instance Zakaznik_A
[PE1-ospf-2]import-route bgp

[PE1]ospf 3 vpn-instance Zakaznik_B
[PE1-ospf-3]import-route bgp
```

8.2.2 Konfigurácia smerovača PE2

Obdobne ako pri konfigurácii smerovača PE1 bolo nutné na začiatku vytvoriť jednotlivé vrf inštancie pre oboch zákazníkov, priradiť im RD a taktiež aj RT, ktorý bol na Huawei smerovači označený ako `vpn-target`.

```
PE2(config)#ip vrf Zakaznik_A
PE2(config-vrf)#rd 1:100
PE2(config-vrf)#route-target export 1:100
PE2(config-vrf)#route-target import 1:100

PE2(config)#ip vrf Zakaznik_B
PE2(config-vrf)#rd 1:200
PE2(config-vrf)#route-target export 1:200
PE2(config-vrf)#route-target import 1:200
```

Následne je nutné vytvorené vrf inštancie priradiť fyzickým rozhraniam hraničného smerovača. Obdobne ako u Huawei smerovača, aj u Cisco smerovača sa priradením vrf inštancie na rozhranie zmaže jeho IP konfigurácia a preto je dobré konfigurovať IP až po priradený vrf inštancie.

```
PE2(config)#interface FastEthernet0/1
PE2(config-if)#ip vrf forwarding Zakaznik_A
PE2(config-if)#ip address 10.0.0.21 255.255.255.252
PE2(config-if)#description PE2-CE3
PE2(config-if)#no shut

PE2(config)#interface Serial0/1/0
PE2(config-if)#ip vrf forwarding Zakaznik_B
PE2(config-if)#ip address 10.0.0.25 255.255.255.252
PE2(config-if)#description PE2-CE4
PE2(config-if)#clock rate 125000
PE2(config-if)#no shut
```

Po priradený vrf inštancií jednotlivým rozhraniam bolo potrebné nakonfigurovať OSPF procesy pre oboch zákazníkov. Oproti konfigurácii na Huawei smerovači je na Cisco smerovači nutné explicitne priradiť OSPF procesu router ID, v prípade že máme viac OSPF procesov.

```
PE2(config)#router ospf 2 vrf Zakaznik_A
PE2(config-router)#router-id 2.2.2.2
PE2(config-router)#network 10.0.0.20 0.0.0.3 area 0

PE2(config)#router ospf 3 vrf Zakaznik_B
PE2(config-router)#router-id 3.3.3.3
PE2(config-router)#network 10.0.0.24 0.0.0.3 area 0
```

Pre naviazanie BGP väzby s protiľahlým smerovačom PE1 je nutné použiť rovnaké značenie BGP autonómneho systému, v tomto prípade 1. Väzba bola naviazaná z rozhrania Loopback0. Obdobne ako u smerovača PE1, nie je nutné BGP susedovi špecifikovať akú rodinu adries podporujeme.

```
PE2(config)#router bgp 1
PE2(config-router)#neighbor 192.168.0.1 remote-as 1
PE2(config-router)#neighbor 192.168.0.1 update-source Loopback0
PE2(config-router)#address-family ipv4
PE2(config-router-af)#no synchronization
PE2(config-router-af)#no neighbor 192.168.0.1 activate
```

Za použitia rovnakého postupu ako pri konfigurácii smerovača PE1 bolo ďalším krokom konfigurácia rodiny adries VPNv4, kde bolo nutné zapnúť zasielanie VPNv4 prefixov príkazom `activate` a predávanie RT parametrov príkazom `send-community both`.

```
PE2(config-router)#address-family vpnv4
```

```
PE2(config-router-af)#neighbor 192.168.0.1 activate
PE2(config-router-af)#neighbor 192.168.0.1 send-community both
```

Posledným krokom konfigurácie bolo zabezpečiť redistribúciu OSPF procesov oboch zákazníkov do MP-BGP a opačne redistribúciu z MP-BGP do oboch OSPF procesov. Pre redistribúciu priamo pripojených podsietí, teda PE2-CE3 u zákazníka A a PE2-CE4 u zákazníka B slúži na Cisco smerovači príkaz `redistribute connected`.

```
PE2(config-router)#address-family ipv4 vrf Zakaznik_A
PE2(config-router-af)#redistribute connected
PE2(config-router-af)#redistribute ospf 2 vrf Zakaznik_A
PE2(config-router-af)#no synchronization

PE2(config-router)#address-family ipv4 vrf Zakaznik_B
PE2(config-router-af)#redistribute connected
PE2(config-router-af)#redistribute ospf 3 vrf Zakaznik_B
PE2(config-router-af)#no synchronization


PE2(config)#router ospf 2 vrf Zakaznik_A
PE2(config-router)#redistribute bgp 1 subnets

PE2(config)#router ospf 3 vrf Zakaznik_B
PE2(config-router)#redistribute bgp 1 subnets
```

8.3 Overenie funkcionality technológie MPLS VPN

Prvým krokom pri overovaní funkcionality MPLS VPN bolo overenie samotného MPLS v sieti poskytovateľa. Funkčnosť MPLS sa dala jednoducho overiť výpisom LFIB tabuľky na hraničnom smerovači. Na obrázku 22 je možné vidieť výpis vnútorných značiek, ktoré smerovač PE1 zvolil pre redistribuované IP prefixy zákazníka B.

```
[PE1]display mpls lsp vpn-instance Zakaznik_B
------------------------------------------------------------------------------
                LSP Information: BGP  LSP
------------------------------------------------------------------------------
FEC                In/Out Label  In/Out IF                      Vrf Name
10.0.0.16/30       1074/NULL     -/-                           Zakaznik_B
192.168.7.1/32     1075/NULL     -/-                           Zakaznik_B
192.168.5.0/24     1076/NULL     -/-                           Zakaznik_B
```

Obrázek 22: Výpis LFIB tabuľky VRF inštancie zákazníka B na smerovači PE1

Ďalším krokom bolo overenie, či sa IP prefixy daného zákazníka úspešne dostali z jednej pobočky na druhú pobočku. Na obrázku 23 je možné vidieť smerovaciu tabuľku z hraničného smerovača zákazníka A na pobočke 1. Prefixy náležia druhej pobočke zákazníka A sa smerovač naučil

pomocou protokolu OSPF. Jedná sa o prefixy 10.0.0.20/30 , 192.168.2.0/24 a 192.168.4.1/32. Ostatné prefixy, okrem tých ktoré sú generované automaticky (prefixy s maskami /32 a /8) náležiace pobočke A sa pomocou protokolu OSPF distribuujú na smerovač PE1.

```
[Huawei]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.12/30  Direct  0    0           D   10.0.0.14       GigabitEthernet0/0/0
      10.0.0.14/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
      10.0.0.15/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
      10.0.0.20/30  O_ASE   150  1           D   10.0.0.13       GigabitEthernet0/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D   192.168.1.1     GigabitEthernet0/0/1
    192.168.1.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
    192.168.2.0/24  O_ASE   150  2           D   10.0.0.13       GigabitEthernet0/0/0
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     LoopBack0
    192.168.3.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
  192.168.3.255/32  Direct  0    0           D   127.0.0.1       LoopBack0
    192.168.4.1/32  O_ASE   150  2           D   10.0.0.13       GigabitEthernet0/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Obrázek 23: Smerovacia tabuľka zákazníckeho smerovača CE1

Prefixy, ktoré smerovač PE1 príjme od smerovača CE1 sa vložia, do VRF smerovacej tabuľky zákazníka A, pretože na rozhraní smerovača PE1, ku ktorému je smerovač CE1 pripojený, je nakonfigurovaná VRF inštancia zákazníka A. Smerovacia tabuľka VRF zákazníka A na smerovači PE1 je zobrazená na obrázku 24.

```
[PE1]display ip routing-table vpn-instance Zakaznik_A
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Zakaznik_A
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.0.0.12/30  Direct  0    0           D   10.0.0.13       GigabitEthernet0/0/0
      10.0.0.13/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
      10.0.0.15/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/0
      10.0.0.20/30  IBGP    255  0          RD   192.168.0.4     GigabitEthernet0/0/1
    192.168.1.0/24  OSPF    10   2           D   10.0.0.14       GigabitEthernet0/0/0
    192.168.2.0/24  IBGP    255  2          RD   192.168.0.4     GigabitEthernet0/0/1
    192.168.3.1/32  OSPF    10   1           D   10.0.0.14       GigabitEthernet0/0/0
    192.168.4.1/32  IBGP    255  2          RD   192.168.0.4     GigabitEthernet0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Obrázek 24: Smerovacia tabuľka VRF zákazníka A

Obdobne je tomu tak aj u Zákazníka B, ktorého smerovacie informácie z hraničného smerovača jeho druhej pobočky je možné vidieť na obrázku 25.

```
CE4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.8.0/24 is directly connected, Loopback0
O E2 192.168.5.0/24 [110/3] via 10.0.0.25, 00:13:45, Serial0/1/0
     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.24 is directly connected, Serial0/1/0
O E2    10.0.0.16 [110/1] via 10.0.0.25, 00:13:45, Serial0/1/0
C    192.168.6.0/24 is directly connected, FastEthernet0/0
     192.168.7.0/32 is subnetted, 1 subnets
O E2    192.168.7.1 [110/3] via 10.0.0.25, 00:13:45, Serial0/1/0
```

Obrázek 25: Smerovacia tabuľka zákazníckeho smerovača CE4

Prefixy, ktoré smerovač CE4 propaguje smerovači PE2 sú zase uložené do VRF smerovacej tabuľky zákazníka B, ktorá je zobrazená na obrázku 26.

```
PE2#show ip route vrf Zakaznik_B

Routing Table: Zakaznik_B
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.8.0/32 is subnetted, 1 subnets
O       192.168.8.1 [110/782] via 10.0.0.26, 00:12:16, Serial0/1/0
B    192.168.5.0/24 [200/3] via 192.168.0.1, 00:21:37
     10.0.0.0/30 is subnetted, 2 subnets
C       10.0.0.24 is directly connected, Serial0/1/0
B       10.0.0.16 [200/0] via 192.168.0.1, 00:26:07
O    192.168.6.0/24 [110/782] via 10.0.0.26, 00:08:08, Serial0/1/0
     192.168.7.0/32 is subnetted, 1 subnets
B       192.168.7.1 [200/3] via 192.168.0.1, 00:24:07
```

Obrázek 26: Smerovacia tabuľka VRF zákazníka B

Na obrázku 27 je možné vidieť výpis VPNv4 prefixov z BGP procesu, ktoré sú vyobrazené pod RD danej VRF inštancie.

```
PE2#show ip bgp vpnv4 all
BGP table version is 86, local router ID is 192.168.0.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:100 (default for vrf Zakaznik_A)
*>i10.0.0.12/30     192.168.0.1              0    100      0 ?
*> 10.0.0.20/30     0.0.0.0                  0         32768 ?
*>i192.168.1.0      192.168.0.1              3    100      0 ?
*> 192.168.2.0      10.0.0.22                2         32768 ?
*>i192.168.3.1/32   192.168.0.1              2    100      0 ?
*> 192.168.4.1/32   10.0.0.22                2         32768 ?
Route Distinguisher: 1:200 (default for vrf Zakaznik_B)
*>i10.0.0.16/30     192.168.0.1              0    100      0 ?
*> 10.0.0.24/30     0.0.0.0                  0         32768 ?
*>i192.168.5.0      192.168.0.1              3    100      0 ?
*> 192.168.6.0      10.0.0.26              782         32768 ?
*>i192.168.7.1/32   192.168.0.1              3    100      0 ?
*> 192.168.8.1/32   10.0.0.26              782         32768 ?
```

Obrázek 27: Výpis VPNv4 prefixov na smerovači PE2

Prefixy, ktoré sa hraničné smerovače poskytovateľa PE1 a PE2 naučia od hraničných smerovačov zákazníka sú ďalej pomocou OSPF redistribuované do smerovacieho protokolu BGP. Redistribuované sú taktiež spojovacie siete medzi hraničnými smerovačmi poskytovateľa a zákazníka, ktoré sme do redistribúcie pridávali príkazmi `redistribute connected` na Cisco smerovači a `import-route direct` na Huawei smerovači. Ku každému prefixu sa pripojí RD danej VRF inštancie a vzknikne tak VPNv4 prefix. Výpis týchto prefixov je možné vidieť na obrázkoch 27 a 28.

```
[PE1]display bgp vpnv4 all routing-table


BGP Local router ID is 10.0.0.1
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete



Total number of routes from all PE: 14
Route Distinguisher: 1:100


     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.0.0.12/30       0.0.0.0         0                    0      ?
*>   10.0.0.13/32       0.0.0.0         0                    0      ?
*>i  10.0.0.20/30       192.168.0.4     0          100       0      ?
*>   192.168.1.0        0.0.0.0         3                    0      ?
*>i  192.168.2.0        192.168.0.4     2          100       0      ?
*>   192.168.3.1/32     0.0.0.0         2                    0      ?
*>i  192.168.4.1/32     192.168.0.4     2          100       0      ?

Route Distinguisher: 1:200


     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.0.0.16/30       0.0.0.0         0                    0      ?
*>   10.0.0.17/32       0.0.0.0         0                    0      ?
*>i  10.0.0.24/30       192.168.0.4     0          100       0      ?
*>   192.168.5.0        0.0.0.0         3                    0      ?
*>i  192.168.6.0        192.168.0.4     782        100       0      ?
*>   192.168.7.1/32     0.0.0.0         3                    0      ?
*>i  192.168.8.1/32     192.168.0.4     782        100       0      ?
```

Obrázek 28: Výpis VPNv4 prefixov na smerovači PE1

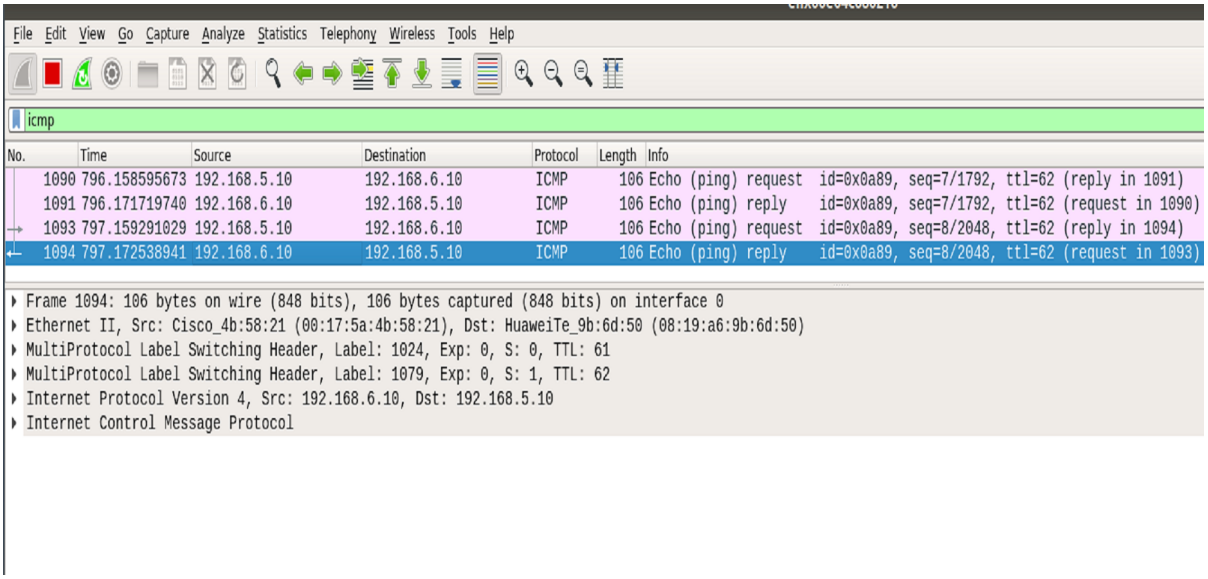
Jednotlivé VPNv4 prefixy sú následne hraničným smerovačom poskytovateľa zasielané na druhý hraničný smerovač poskytovateľa pomocou protokolu MP-BGP. Napríklad VPNv4 prefixy náležiace zákazníkovi A sú zo smerovača PE1 zasielané pomocou MP-BGP na smerovač PE2 vo formáte 1:100:192.168.1.0/24, 1:100:192.168.3.1/32 a 1:100:10.0.0.12/30. Smerovač PE2 obdrží BGP aktualizáciu, ktorá obsahuje VPNv4 prefix, vnútornú MPLS značku pre daný IP prefix a RT Export. Tieto informácie sú zobrazené na obrázku 27, pričom prefixy naúčené pomocou MP-BGP(iBGP) sú označené písmenom "i". Pomocou hodnoty RT Export je smerovač schopný zistiť, do ktorej smerovacej tabuľky sa majú dané prefixy zapísať. Napríklad ak sa hodnota RT Import v danej VRF zhoduje s hodnotou RT Export v prijatom prefixe, tak sa prefix zapíše do tejto VRF tabuľky. Predtým než sa prefix zapíše do VRF tabuľky sa hodnota RD z prefixu odstráni. Prefixy sú následne smerovačom PE2 redistribuované do príslušného OSPF procesu daného zákazníka a potom pomocou OSPF propagované na hraničné smerovače zákazníckych pobočiek.

Ďalším krokom pri testovaní správnej funkcionality MPLS VPN bolo overenie samotnej konektivity medzi pobočkami daného zákazníka. Testovanie bolo uskutočnené pomocou príkazu `ping` zo stanice náležiacej prvej pobočke zákazníka B smerom na stanicu náležiacu druhej pobočke Zákazníka B. Úspešný výstup príkazu `ping` je zachytený na obrázku 29.

```
student@pc14:~$ ifconfig enx00e04c680201
enx00e04c680201: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.10  netmask 255.255.255.0  broadcast 192.168.5.255
        ether 00:e0:4c:68:02:01  txqueuelen 1000  (Ethernet)
        RX packets 1114  bytes 291596 (291.5 KB)
        RX errors 0  dropped 213  overruns 0  frame 0
        TX packets 546  bytes 59091 (59.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

student@pc14:~$ ping 192.168.6.10
PING 192.168.6.10 (192.168.6.10) 56(84) bytes of data.
64 bytes from 192.168.6.10: icmp_seq=1 ttl=58 time=14.5 ms
64 bytes from 192.168.6.10: icmp_seq=2 ttl=58 time=14.2 ms
64 bytes from 192.168.6.10: icmp_seq=3 ttl=58 time=14.3 ms
64 bytes from 192.168.6.10: icmp_seq=4 ttl=58 time=14.2 ms
64 bytes from 192.168.6.10: icmp_seq=5 ttl=58 time=14.0 ms
64 bytes from 192.168.6.10: icmp_seq=6 ttl=58 time=14.1 ms
64 bytes from 192.168.6.10: icmp_seq=7 ttl=58 time=14.3 ms
64 bytes from 192.168.6.10: icmp_seq=8 ttl=58 time=14.2 ms
^C
--- 192.168.6.10 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7009ms
rtt min/avg/max/mdev = 14.097/14.267/14.540/0.175 ms
```

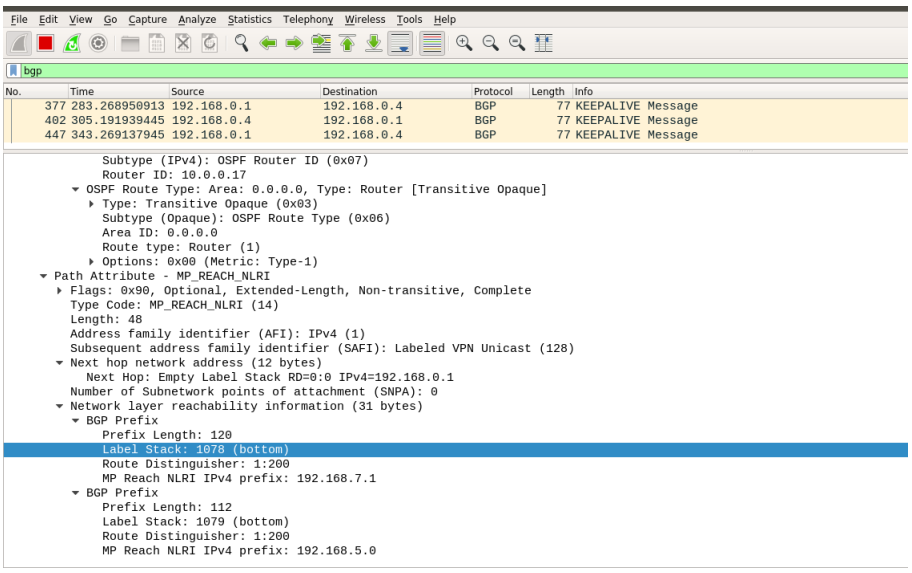
Obrázek 29: Úspešný výstup príkazu `ping` na jednej zo zákazníckych staníc

Toto ICMP spojenie bolo taktiež zachytené pomocou tretej stanice, pripojenej pomocou HUB zariadenia medzi smerovačmi P1 a P2 v programe Wireshark a je ho možné vidieť na obrázku 30.



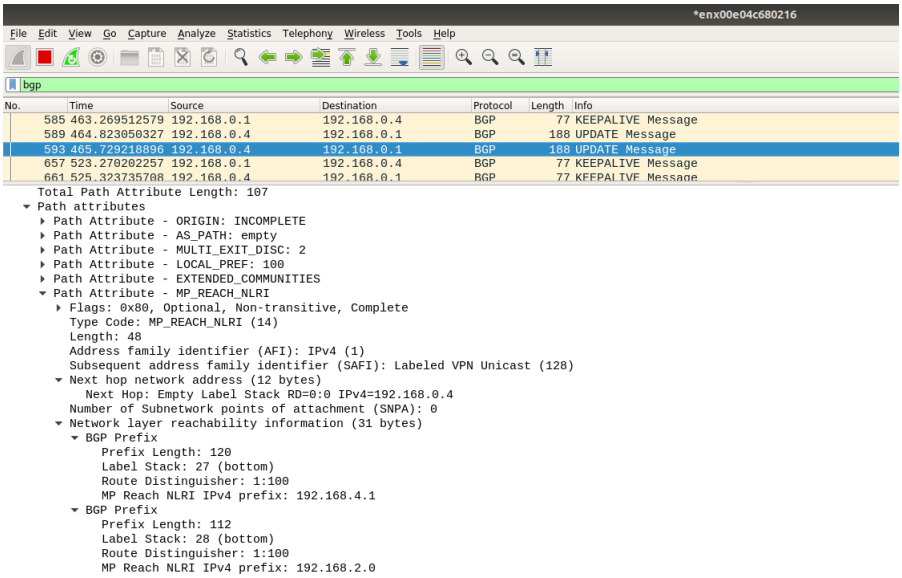
Obrázek 30: ICMP správa zachytená v programe Wireshark

Po úspešnom otestovaní konektivity medzi zákazníckymi pobočkami nasledovalo ešte odchytenie BGP aktualizačných správ v programe Wireshark. Najprv bola zo smerovača PE1 odpojená a následne znova pripojená pobočka 1 zákazníka B, následkom čoho zasielal smerovač PE1 BGP aktualizáciu smerovaču PE2 s novými VPNv4 prefixmi. Táto správa je zachytená na obrázku 31.



Obrázek 31: BGP aktualizačná správa zo smerovača PE1 zachytená v programe Wireshark

Následne bola zo smerovača PE2 odpojená a opäť pripojená druhá pobočka zákazníka A, následkom čoho zasielal smerovač PE2 smerovači PE1 BGP aktualizačnú správu o nových VPNv4 prefixoch. Táto správa je zachytená na obrázku 32.



Obrázek 32: BGP aktualizačná správa zo smerovača PE2 zachytená v programe Wireshark

Na obrázkoch 31 a 32 ja taktiež možné vidieť vnútorné MPLS značky, ktoré hraničné smerovače PE1 a PE2 priradili daným IP prefixom.

9 Porovnanie platforiem Cisco a Huawei

Pri vypracovávaní diplomovej práce boli použité dve rôzne sieťové platformy a to Cisco a Huawei. Zatiaľ čo Cisco zariadenia využívali operačný systém IOS verzie 12.4 u smerovačov a verzie a 12.2 u prepínačov, Huawei zariadenia využívali operačný systém Versatile Routing Platform Software(VRP Software) s verziou 5.120. Pri konfigurácii jednotlivých virtualizačných technológií neboli pomimo konfiguračnej syntaxe medzi platformami žiadne veľké rozdieli, avšak našlo sa ich pár na ktoré sa oplatí poukázať.

Na prvý rozdiel medzi platformami Cisco a Huawei užívateľ natrafí hneď pri začiatku konfigurácie smerovača od spoločnosti Huawei. Po štarte Huawei smerovača je užívateľ ešte pred vstupom do systému vyzvaný ku nastaveniu prístupového hesla a ku nastaveniu funkcie auto-config. Funkcia auto-config na Huawei smerovačoch slúži ku sťahovaniu systémovej verzie, aktualizačných súborov alebo konfigurácie automaticky po štarte systému. Táto funkcia nachádza svoje uplatnenie hlavne vo väčších sieťach, v prípade kedy je nutné do siete naraz implementovať väčšie množstvo smerovačov. Miesto toho aby sa každý zo smerovačov konfiguroval separátne, si pomocou funkcie auto-config môžu smerovače automaticky stiahnuť konfiguráciu alebo rôzne aktualizácie z definovaného serveru.

```
Please configure the login password (maximum length 16)
Enter password:huawei
Confirm password:huawei

Warning: Auto-Config is working. Before configuring the device, stop
Auto-Config. If you perform configurations when Auto-Config is running, the
DHCP, routing, DNS, and VTY configurations will be lost. Do you want to
stop Auto-Config? [y/n]: no
```

Pri konfigurácii technológií ako EtherChannel alebo VLAN na prepínačoch Cisco a Huawei, sa môže užívateľ stretnúť hneď s niekoľkými rozdielmi. Prvý z týchto rozdielov je pri konfigurácii trunk rozhraní na prepínačoch. Zatiaľ čo u Cisco prepínačoch je nutné definovať aký enkapsulačný protokol sa bude používať, Huawei prepínače používajú automaticky enkapsulačný protokol dot1q. Cisco prepínače od rady 2970 a vyššie podporujú taktiež cisco proprietárny enkapsulačný protokol ISL(Inter-Switch-Link) a je nutné zvoliť, ktorý sa má používať. Ďalší z rozdielov spočíval v časovej obtiažnosti konfigurácie technológie EtherChannel. Zatiaľ čo u Huawei prepínača stačilo nakonfigurovať len virtuálne rozhranie Eth-Trunk a fyzické potom už len ku tomuto virtuálnemu rozhraniu priradiť, tak u Cisco prepínača bolo nutné každé rozhranie konfigurovať explicitne. U Huawei prepínača taktiež nie je nutné definovať v akom móde má pracovať LACP, ktoré potom automaticky funguje v móde active, zatiaľ čo u Cisco prepínača je nutné definovať v akom móde má LACP pracovať.

Pri konfigurácii technológie VRRP bolo zaujímavé zistenie, že Cisco zariadenia podporujú VRRPv3, ktoré oproti VRRPv2 podporuje IPv6, až od systému IOS verzie 15 a vyššie. Cisco smerovač 2800 s verziou IOS 12.4, ktorý bol použitý pri konfigurácii tejto technológie, teda VRRPv3 nepodporoval. Naproti tomu smerovač Huawei AR3200, ktorý bol taktiež použitý pri tejto implementácii, VRRPv3 podporoval.

Konfigurácia technológie MPLS VPN prebiehala z hľadiska jednotlivých krokov, ak neberieme v úvahu konfiguračnú syntax, takmer rovnako. U Cisco smerovačov bolo nutné zapnutie Cisco proprietárnej technológie CEF, pretože MPLS sa opiera o podkladovú štruktúru a logiku expresného zasielania. Ďalším zaujímavým poznatkom je rozdiel v číslovaní MPLS rámcov u oboch smerovačov. Zatiaľ čo Huawei smerovač PE1 tieto značky generuje od hodnoty 1024 tak Cisco smerovač PE2 tieto značky generuje od hodnoty 16, čo svojím spôsobom v prípade problému v sieti zjednodušuje administrátorovi prácu z hľadiska identifikácie.

10 Záver

Cieľom tejto diplomovej práce bolo popísať rôzne virtualizačné technológie bežne používané v praxi, následne ich implementovať v laboratórnych podmienkach za využitia platforiem Cisco a Huawei, preukázať kompatibilitu týchto dvoch platforiem a vzájomne ich porovnať.

Pri vypracovávaní diplomovej práce bolo pri technológii MPLS VPN dohromady použitých osem smerovačov, z toho päť smerovačov bolo značky Cisco série 2801 a využívali operačný systém IOS verzie 12.4. Zvyšné tri smerovače boli značky Huawei a jednalo sa o modely AR1220, AR2200 a AR3200. Tieto smerovače využívali operačný systém od spoločnosti Huawei, Versatile Routing Platform Software(VRP Software).Pri konfigurácii technológií EtherChannel, SVI a InterVLAN routing boli použité dva prepínače, jeden značky Cisco Catalyst 3560, ktorý využíval IOS verzie 12.2 a Huawei S5600, ktorý využíval operačný systém VRP Software. Pri konfigurácií technológie VRRP boli použité smerovače Huawei AR3200 a Cisco 2801.

Virtualizačné technológie boli testované v troch konfiguračných schémach. Prvá schéma zahrňovala technológie VLAN, EtherChannel, SVI a InterVLAN smerovanie a simulovala ich bežné použitie v praxi. V druhej schéme bola testovaná technológia VRRP pri jej najzákladnejšej funkcionalite za použitia dvoch smerovačov a jednej VRRP skupiny. Tretia konfiguračná schéma znázorňovala možnosť využitia technológie MPLS VPN poskytovateľom, pri prepájaní zákazníckych pobočiek viacerých zákazníkov.

Pri konfigurácii jednotlivých virtualizačných technológií neboli pomimo konfiguračnej syntaxe rozdielnych platforiem a rozdielov spomenutých v kapitole 10, žiadne veľké rozdiely. U všetkých implementovaných virtualizačných technológií bola preukázateľná správna funkcionalita a táto práca teda potvrdzuje, že nasadenie platforiem Cisco a Huawei v spoločnej platformovo nehomogénnej sieti pri implementácii virtualizačných technológií, ktorými sa táto práca zaoberá, je realizovateľné. Prípadný administrátor siete teda môže stávajúcu počítačovú sieť postavenú na Cisco platforme rozšíriť o zariadenia značky Huawei, prípadne naopak rozšíriť počítačovú sieť založenú na platforme Huawei o Cisco zariadenia.

Literatura

[1] Ing. Fík, Antonín, *Diplomová práca - Virtuální privátní síť v prostředí MPLS technologie*

[2] Eversed, Sean, *Under the Hood of MPLS VPNs* [online]. Dostupné z: `https://learningnetwork.cisco.com/blogs/community_cafe/2015/03/12/under-the-hood-of-mpls-vpns-part-1-by-sean-evershed`

[3] *Configuring VRF-lite* [online]. Dostupné z: `https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/vrf.pdf`

[4] Stretch, Jeremy, *Intro to VRF lite* [online]. Dostupné z: `http://packetlife.net/blog/2009/apr/30/intro-vrf-lite/`

[5] Grygarek, Petr, *MPLS a VPN* [online]. Dostupné z: `http://www.cs.vsb.cz/grygarek/TPS/MPLS/MPLS-VPN-config/MPLS-lab.pdf`

[6] Grygarek, Petr, *Směrovací protokol BGP* [online]. Dostupné z: `http://www.cs.vsb.cz/grygarek/SPS/lect/BGP/BGP.html`

[7] *Huawei documentation* [online]. Dostupné z: `https://support.huawei.com`

[8] Hlozák, Martin, *Diplomová práca - Návrh sítě MPLS s využitím směrovačů Huawei*

[9] Machník, Petr, *Širokopásmové sítě pro integrovanou výuku VUT a VŠB-TUO* [online]. Dostupné z: `https://lms.vsb.cz/pluginfile.php/647397/mod_resource/content/4/Širokopásmovésítě.pdf.pdf`

[10] *MPLS AToM,L2TPv3 and Interworking IP Pt4 AToM* [online]. Dostupné z: `https://packetized.wordpress.com/2010/08/21/mpls-atoml2tpv3-and-interworking-ip-pt4-a`

[11] Ševčík, Libor, *Bakalárska práca - MODEL SÍŤOVÉHO PROSTŘEDÍ VYUŽÍVAJÍCÍ REDUNDANTNÍ PROTOKOL*

A EtherChannel, SVI a InterVLAN routing - Skrátený výpis konfigurácie prepínača Cisco Catalyst 3560

```
Building configuration...

Current configuration : 2033 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
vtp mode transparent
ip subnet-zero
ip routing
!
vlan internal allocation policy ascending
!
vlan 2-3
!
vlan 200
 name 200
!
vlan 300
 name 300
!
vlan 400
 name 400
!
interface Port-channel1
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 200,300,400
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 200,300,400
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 200,300,400
 switchport mode trunk
 channel-group 1 mode active
!
interface FastEthernet0/3
 switchport access vlan 300
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan300
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan400
 ip address 10.0.0.1 255.255.255.0
!
ip classless
ip route 192.168.0.0 255.255.255.0 10.0.0.2
ip http server
ip http secure-server
!
control-plane
!
line con 0
line vty 5 15
!
```

```
end
```

B EtherChannel, SVI a InterVLAN routing - Skrátený výpis konfigurácie prepínača Cisco Catalyst 3560

```
!Software Version V200R005C00SPC300
#
sysname Quidway
#
vlan batch 200 300 400
#
undo authentication unified-mode
#
undo http server enable
undo http secure-server enable
#
vlan 200
 name 200
vlan 300
 name 300
vlan 400
 name 400
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %@%@rGeR-|MjFC<,Hx66|XCNyy5h%@%@
 local-user admin service-type http
#
interface Vlanif1
#
interface Vlanif200
 ip address 192.168.0.1 255.255.255.0
#
interface Vlanif400
 ip address 10.0.0.2 255.255.255.0
#
interface Eth-Trunk1
```

```
 port link-type trunk
 port trunk allow-pass vlan 200 300 400
 mode lacp
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
ip route-static 192.168.1.0 255.255.255.0 10.0.0.1
#
user-interface con 0
 authentication-mode password
 set authentication password cipher @%@%"\z)1}HU^UsAdSSU11oWyy5Rk;9eI:ul.8,_.aR)i3PBy5Uy@
user-interface vty 0 4
user-interface vty 16 20
#
return
[Quidway]
```

C VRRP - Skrátený výpis konfigurácie smerovača Cisco 2801s

```
Building configuration...

Current configuration : 1323 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot system flash:c2801-advipservicesk9-mz.124-22.T.bin
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
dot11 syslog
ip source-route
!
ip cef
!
interface FastEthernet0/1
 ip address 192.168.0.3 255.255.255.0
 duplex auto
 speed auto
 vrrp 1 ip 192.168.0.1
 vrrp 1 timers learn
 vrrp 1 priority 90
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
```

```
end
```

D VRRP - Skrátený výpis konfigurácie smerovača Huawei AR3200

```
[V200R003C00SPC200]
#
 sysname R2
#
 snmp-agent local-engineid 800007DB030819A69A8275
 snmp-agent
#
cwmp
 cwmp cpe connect retry 0
#
 http timeout 3
#
 drop illegal-mac alarm
#
vrrp recover-delay 2
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
firewall zone Local
 priority 128
#
interface GigabitEthernet0/0/1
 ip address 192.168.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.0.1
 vrrp vrid 1 priority 120
 vrrp vrid 1 timer advertise 2
#
#
user-interface con 0
 authentication-mode password
```

```
 set authentication password cipher %$%$m:}(5Y#YT)7W'l,g<4MP,.l<O=v9B]w\t.5z:..a]YZ'.l~,%
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
return
```

E MPLS VPN - Skrátený výpis konfigurácie smerovača PE1 (Huawei AR3200)

```
[V200R003C00SPC200]
#
 sysname PE1
#
#
ip vpn-instance Zakaznik_A
 ipv4-family
  route-distinguisher 1:100
  vpn-target 1:100 export-extcommunity
  vpn-target 1:100 import-extcommunity
#
ip vpn-instance Zakaznik_B
 ipv4-family
  route-distinguisher 1:200
  vpn-target 1:200 export-extcommunity
  vpn-target 1:200 import-extcommunity
#
mpls lsr-id 192.168.0.1
mpls
 lsp-trigger all
#
mpls ldp
#
#
interface GigabitEthernet0/0/0
 description PE1-CE1
 ip binding vpn-instance Zakaznik_A
 ip address 10.0.0.13 255.255.255.252
#
interface GigabitEthernet0/0/1
 description PE1->P1
 ip address 10.0.0.1 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/2
```

```
 description PE1-CE2
 ip binding vpn-instance Zakaznik_B
 ip address 10.0.0.17 255.255.255.252
#
interface LoopBack0
 ip address 192.168.0.1 255.255.255.255
#
bgp 1
 peer 192.168.0.4 as-number 1
 peer 192.168.0.4 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  undo peer 192.168.0.4 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 192.168.0.4 enable
 #
 ipv4-family vpn-instance Zakaznik_A
  import-route direct
  import-route ospf 2
 #
 ipv4-family vpn-instance Zakaznik_B
  import-route direct
  import-route ospf 3
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 192.168.0.1 0.0.0.0
#
ospf 2 vpn-instance Zakaznik_A
 import-route bgp
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
#
ospf 3 vpn-instance Zakaznik_B
 import-route bgp
```

```
 area 0.0.0.0
  network 10.0.0.16 0.0.0.3
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$n$]">a/cFK‘8<><6{,3;,"S!icVvO+}x#H=\_&<"W^G("S$,%
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
return
[PE1]
```

F MPLS VPN - Skrátený výpis konfigurácie smerovača P1 (Huawei AR2200)

```
V200R005C20SPC200]
#
 sysname P1
#
#
interface GigabitEthernet0/0/0
#
interface GigabitEthernet0/0/1
 ip address 10.0.0.2 255.255.255.252
 description P1->PE1
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/2
 description P1->P2
 ip address 10.0.0.5 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 192.168.0.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.3
  network 10.0.0.4 0.0.0.3
  network 192.168.0.2 0.0.0.0
#
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %@%@pIeO.#Yma7}1&(R"yJs,,"6Xp-)p*gBhm=pGIxMvUCBS"6[,%
user-interface vty 0 4
#
wlan ac
#
```

```
voice
 #
 diagnose
#
return
```

G MPLS VPN - Skrátený výpis konfigurácie smerovača PE2 (Cisco 2801s)

```
Building configuration...

Current configuration : 2513 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
ip cef
ip vrf Zakaznik_A
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf Zakaznik_B
 rd 1:200
 route-target export 1:200
 route-target import 1:200
!
mpls label protocol ldp
!
interface Loopback0
 ip address 192.168.0.4 255.255.255.255
!
interface FastEthernet0/0
 description PE2->P2
 ip address 10.0.0.10 255.255.255.252
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 description PE2->CE3
```

```
 ip vrf forwarding Zakaznik_A
 ip address 10.0.0.21 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/1/0
 description PE2->CE4
 ip vrf forwarding Zakaznik_B
 ip address 10.0.0.25 255.255.255.252
 clock rate 125000
!
router ospf 2 vrf Zakaznik_A
 router-id 2.2.2.2
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 10.0.0.20 0.0.0.3 area 0
!
router ospf 3 vrf Zakaznik_B
 router-id 3.3.3.3
 log-adjacency-changes
 redistribute bgp 1 subnets
 network 10.0.0.24 0.0.0.3 area 0
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.8 0.0.0.3 area 0
 network 192.168.0.4 0.0.0.0 area 0
!
router bgp 1
 bgp log-neighbor-changes
 neighbor 192.168.0.1 remote-as 1
 neighbor 192.168.0.1 update-source Loopback0
 !
 address-family ipv4
  no neighbor 192.168.0.1 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
```

```
 address-family vpnv4
  neighbor 192.168.0.1 activate
  neighbor 192.168.0.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf Zakaznik_B
  redistribute connected
  redistribute ospf 3 vrf Zakaznik_B
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf Zakaznik_A
  redistribute connected
  redistribute ospf 2 vrf Zakaznik_A
  no synchronization
 exit-address-family
!
mpls ldp router-id Loopback0 force
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

H MPLS VPN - Skrátený výpis konfigurácie smerovača P2 (Cisco 2801s)

```
Building configuration...

Current configuration : 1370 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2
!
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 192.168.0.3 255.255.255.255
!
interface FastEthernet0/0
 description P2->PE2
 ip address 10.0.0.9 255.255.255.252
 duplex auto
 speed auto
 mpls ip
!
interface FastEthernet0/1
 description P2->P1
 ip address 10.0.0.6 255.255.255.252
 duplex auto
 speed auto
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.4 0.0.0.3 area 0
 network 10.0.0.8 0.0.0.3 area 0
```

```
 network 192.168.0.3 0.0.0.0 area 0
!
mpls ldp router-id Loopback0 force
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

I MPLS VPN - Skrátený výpis konfigurácie smerovača CE1 (Huawei AR1220)

```
[V200R003C00SPC200]
#
 sysname CE1
#
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$=i~>Xp&aY+*2cEVcS-A23Uwe%$%$
 local-user admin service-type http
#
interface Eth-Trunk1
 mode lacp-static
#
interface Ethernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/0
 description CE1->PE1
 ip address 10.0.0.14 255.255.255.252
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack0
 ip address 192.168.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.0.0.12 0.0.0.3
  network 192.168.1.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
```

```
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%$v&T6<hWEAI$m~(4hh)}',.)e%-H>7&&RG7])%z!:BL~!.)h,%
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
return
```

J MPLS VPN - Skrátený výpis konfigurácie smerovača CE2 (Cisco 2801s)

```
Building configuration...

Current configuration : 1298 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE2
!
ip cef
!
interface Loopback0
 ip address 192.168.7.1 255.255.255.0
!
interface FastEthernet0/0
 description CE2->PE1
 ip address 10.0.0.18 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.16 0.0.0.3 area 0
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
!
line con 0
line aux 0
line vty 0 4
```

```
 login
!
end
```

K MPLS VPN - Skrátený výpis konfigurácie smerovača CE3 (Cisco 2801s)

```
Building configuration...

Current configuration : 1283 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE3
!
ip cef
!
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description CE3->PE2
 ip address 10.0.0.22 255.255.255.252
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.20 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
line con 0
line aux 0
line vty 0 4
```

```
 login
!
end
```

L MPLS VPN - Skrátený výpis konfigurácie smerovača CE4 (Cisco 2801s)

```
Building configuration...

Current configuration : 1279 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE4
!
ip cef
!
interface Loopback0
 ip address 192.168.8.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.6.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/1/0
 description CE4->PE2
 ip address 10.0.0.26 255.255.255.252
 no fair-queue
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.24 0.0.0.3 area 0
 network 192.168.6.0 0.0.0.255 area 0
 network 192.168.8.0 0.0.0.255 area 0
!
line con 0
line aux 0
line vty 0 4
 login
```

```
!
end
```